MÜHENDİSLİK FAKÜLTESİ

SİBER GÜVENLİK

TEZSİZ YÜKSEK LİSANS DÖNEM PROJESİ

KURUMSAL BİR AĞ SİSTEMİNİN AÇIK KAYNAKLI YAZILIMLAR KULLANILARAK MODELLENMESİ VE SALDIRI TESPİTİ

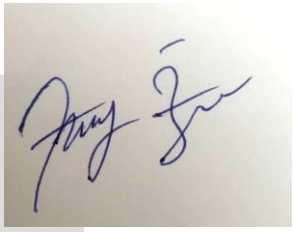
HAZIRLAYAN
TUNCAY ÖZER

DANIŞMAN ÖĞRETİM ÜYESİ
PROF.DR. İBRAHİM ÖZÇELİK

2020

ETİK İLKELERE UYGUNLUK BEYANI

Dönem proje yazma sürecinde bilimsel ve etik ilkelere uyduğumu, yararlandığım tüm kaynakları kaynak gösterme ilkelerine uygun olarak kaynakçada belirttiğimi ve bu bölümler dışındaki tüm ifadelerin şahsıma ait olduğunu beyan ederim.



Tuncay ÖZER

KURUMSAL BİR AĞ SİSTEMİNİN AÇIK KAYNAKLI YAZILIMLAR KULLANILARAK MODELLENMESİ VE SALDIRI TESPİTİ

Tuncay ÖZER

AHMET YESEVİ ÜNİVERSİTESİ

SİBER GÜVENLİK

2020

ÖZET

Günümüzde hayatımızın her alanına giren kişisel bilgisayarlar, mobil tablet, telefon, giyilebilir teknolojilerinin artması, dijital ortamda oluşturulan verilerin anlamlandırılarak saklanması, gizlilik, bütünlük ve kullanılabilirliğinin sağlanması siber saldırı yöntemlerinden korunması amacıyla siber güvenlik tekniklerinin uygulanması bir ihtiyaç olmuştur. Kişisel ve kurumsal anlamda siber saldırıları bertaraf edebilecek sistemler ihtiyaca, tespit ve saldırı yöntemine göre geliştirilmektedir. Siber güvenlik sistemlerinde güvenlik duvarları, saldırı tespit, sanal ağ, ağ trafik analizleri, olay kaydediciler, zafiyet tarayıcıları, kaynak kod güvenlik analizleri, parola kontrol gibi yazılımlardır. Bu yazılımlar, ücretli olarak dağıtımı yapılabildiği gibi ücretsiz olarak açık kaynak desteği sunan platformlar da bulunmaktadır. Bu proje çalışmasının amacı açık kaynak yazılımlarla kurumsal bir ağ sisteminin açık kaynak yazılımlar kullanarak modellenmesi ve saldırı tespitinin yapılmasıdır. Bu kapsamda en çok kullanılan açık kaynak kodlu yazılımlar hakkında genel bilgiler verilerek hedef doğrultusunda kurulumları gerçekleştirmektir. Sonuçlar çalışma sonunda sonuç ve öneriler kısmında paylaşılmıştır.

Anahtar Kelimeler: açık kaynak, kurumsal ağ sistemi, ağ güvenliği, saldırı tespiti

Danışman: Prof. Dr. İbrahim ÖZÇELİK

MODELING AND ATTACK DETECTION OF A CORPORATE NETWORK SYSTEM USING OPEN SOURCE SOFTWARE

Tuncay OZER

AHMET YESEVI UNIVERSITY

SYBER SECURITY

2020

ABSTRACT

Today, it has become a necessity to apply cyber security techniques in order to increase personal computers, mobile tablets, phones, wearable technologies that enter into every area of our lives, to make sense of the data created in digital environment, to protect privacy, integrity and usability from cyber attack methods. Systems that can eliminate cyber attacks personally and institutionally are developed according to the need, detection and attack method. In cyber security systems, firewalls are software such as intrusion detection, virtual network, network traffic analysis, event recorders, vulnerability scanners, source code security analysis, password control. These software can be distributed for a fee or there are platforms that offer open source support for free. The purpose of this assignment is to model an enterprise network system with open source software using open source software and to detect attack. In this context, general information about the most used open source software is to provide installations in line with the target. The results are shared in the results and recommendations section at the end of the homework.

Keywords: open source, corporate network system, network security, intrusion detection

Advisor: Prof. İbrahim ÖZÇELİK

İÇİNDEKİLER

ETİK İLKELERE UYGUNLUK BEYANI ii
ÖZET 1
ABSTRACT 2
İÇİNDEKİLER 3
ŞEKİLLER LİSTESİ 5
TABLOLAR LİSTESİ 8
SİMGELER VE KISALTMALAR 9
BÖLÜM I GİRİŞ 10
1.1. Problem 10
1.2. Araştırmanın Amacı 10
1.3. Araştırmanın Önemi 10
1.4. Sayıltılar 11
1.5. Sınırlılıklar 11
1.6. Tanımlar 11
1.6.1.Vmware Sanallaştırma Yazılımı 11
1.6.2. İşletim Sistemleri 12
1.6.3. PfSense 13
1.6.4. Snort 13
BÖLÜM II SALDIRI TESPİT SİSTEMLERİ 14
2.1. Bilgi Güvenliği 14
2.2. Siber Güvenlik 15
2.2. Saldırı Tespit Sistemleri 15
2.3. Açık Kaynak Kodlu Siber Güvenlik Yazılımları 16
2.4. Ağ Topolojisinin Oluşturulması 16
2.5. Vmware Kurulumu ve Yapılandırılması 18
2.5.1. Sanal Makina Oluşturulması 18
2.6. Güvenlik Duvarı Pfsense Kurulumu ve Yapılandırılması 21
2.7. Snort Kurulumu ve Yapılandırılması 27
2.8. Misafir İşletim Sistemlerinin Kurulması 30
BÖLÜM III SİSTEM ENTEGRASYONU VE TEST 32
3.1. Snort Aktif Etme 32
3.2. Model Ağ Sistemine Saldırılar 35
3.2.1. Keşif Saldırıları 35

3.2.1.1. NMAP 35
3.2.2. ATAKLAR 37
3.2.2.1. ACK-PUSH Atak 39
3.2.2.2. UDP Atak 40
3.2.2.3. RST / FIN Atak 42
3.2.2.4. ICMP Atak 42
3.2.2.5. TCP SYN Atak 43
3.2.2.6. Slowloris Session Atak 45
3.2.3.7. Xerxes Yalancı (Fake) Session Atak 47
3.2.2.8. Golden Eye (Altın Göz) Atak 48
3.3. Ek Olarak Yapılabilecek Ataklar 50
3.3.1 Zaman, Ajan adı ve Port Numarası Değiştirme [20] 50
3.3.2.Test Ortamı ve Saldırı 52
3.4. Saldırı Sonuçları 55
BÖLÜM IV BULGULAR VE YORUM 59
4.1. Birinci Araştırma sorusuna ilişkin bulgular 59
4.2. DDoS ve DoS Ataklarına Karşı Alınabilecek Önlemler 59
4.3. Yeni Ataklara Karşılık Bulgular 59
4.4. Atlatma Tekniklerine Karşı Alınabilecek Önlemler 59
BÖLÜM V SONUÇ, TARTIŞMA VE ÖNERİLER 61
5.1. Sonuç 61
5.2. Öneriler 61
KAYNAKÇA 62

ŞEKİLLER LİSTESİ

Şekil 2.1.	Temel Topoloji Şeması Genel Konumlar	17
Şekil 2.2.	Genel Ağ Topolojisi	17
Şekil 2.3.	Yeni Sanal Makine Oluştur Seçimi	18
Şekil 2.4.	Tipik Seçim	19
Şekil 2.5.	Kurulacak Sistemin ISO Dosyasının Seçimi	19
Şekil 2.6.	Kurulacak olan işletim sisteminin konumu ve sanal dosya adının belirlenmesi	20
Şekil 2.7.	Kurulacak sistemin sanal üzerinde kapasitesinin belirlenmesi	20
Şekil 2.8.	Sanal Sistem Konfigürasyonu Listesi	21
Şekil 2.9.	Pfsense ISO dosyası indirme	22
Şekil 2.10.	Pfsense Telif Hakları	23
Şekil 2.11.	Pfsense Hoş Geldiniz Ekranı	23
Şekil 2.12.	Keymap seçenekleri	24
Şekil 2.13.	Disk Bölümleme	24
Şekil 2.14.	Pfsense Kurulum	25
Şekil 2.15.	Manuel Yapılandırma Sorgulama Ekranı	25
Şekil 2.16.	Pfsense Başlangıç ve Yapılandırma Seçenekleri	26
Şekil 2.17.	Pfsense Erişim Ekranı	27
Şekil 2.18.	Pfsense mevcut paketler bölümü	27
Şekil 2.19.	Paketler Listesi	28
Şekil 2.20.	Snort Kurulumu	28
Şekil 2.21.	Snort OinkCode ekranı	29
Şekil 2.22.	Snort Oinkcode Giriş Ekranı	29

Şekil 2.23.	Snort Rule Update İşlemi	30
Şekil 2.24.	Snort Rule Update İşleminin Bitimi	30
Şekil 3.1.	Snort Servisi Seçimi	31
Şekil 3.2.	Wan Network Bacağını Ayarlama-1	32
Şekil 3.3.	Wan Bacağı	32
Şekil 3.4.	Wan Kategorisi Kural Seçimi	33
Şekil 3.5.	Firewall Log Görüntüsü	34
Şekil 3.6.	PfSense Makinasına Nmap Keşfi	36
Şekil 3.7.	Snort Nmap UDP paketlerinin tespiti	37
Şekil 3.8.	Custom Rol Giriş Ekranı	38
Şekil 3.9.	Snort Arayüzü Push Attack	38
Şekil 3.10.	Hping3 paket gönderme	39
Şekil 3.11.	Wireshark ile gönderilen paketler listesi	40
Şekil 3.12.	Snort Güvenlik Duvarı	40
Şekil 3.13.	Internet Information Services web arayüzü	40
Şekil 3.14.	Reset Dos Atak	41
Şekil 3.15.	Wireshark ICMP atakları	42
Şekil 3.16.	Snort ICMP atakları	42
Şekil 3.17.	Ettercap dos_attack	43
Şekil 3.18.	Snort Ettercap Dos Atağı alarmı	43
Şekil 3.19.	Slowloris indirme	44
Şekil 3.20.	Slowloris Atak	44
Şekil 3.21.	Wireshark Slowloris paketleri	45
Şekil 3.22.	Snort Slowloris Alarm	45

Şekil 3.23.	Xerxes uygulamasını github platformundan indirme	46
Şekil 3.24.	Xerxes Atak	46
Şekil 3.25.	Wireshark Xerxes paket gönderme görüntüsü	47
Şekil 3.26.	Snort Xerxes alarmı	47
Şekil 3.27.	GoldenEye uygulamasını github platformundan indirme	48
Şekil 3.28.	GoldenEye Atak.	48
Şekil 3.29.	GoldenEye Snort Alarm.	48
Şekil 3.30.	Örnek Snort Kuralı (https://slideplayer.com/slide/13774900/)	52

TABLOLAR LİSTESİ

Tablo 2.1.	Donanım Özellikleri…….....	16
Tablo 2.2.	Kullanılan Yazılımlar ve Sürüm Numaraları……..	16
Tablo 2.3.	Pfsense için Sanal Makine Özellikleri…….....	22
Tablo 2.5.	Kali Linux ve Windows 10 Pro Sanal Makine Özellikleri…….	31
Tablo 3.1.	Saldırılar…….....	54
Tablo 3.2.	Saldırı Denemeleri ve Sonuçları ……...	55
Tablo 3.3.	Ajan adı değiştirme atlatma tekniği deneme sonuçları……	57
Tablo 3.4.	Port numarası değiştirme atlatma tekniği test sonuçları……..	58

SİMGELER VE KISALTMALAR

IDS	: Intrusion Detection System
SYN	: SYNchronize
TCP/IP	: Transmission Control Protocol / Ip Protocol
IPS	: Intrusion Prevention System
NAT	: Network Adress Translation
NIC	: Network Interface Card
GPL	: General Public License
DHCP	: Dynamic Host Configuration Protocol
SSH	: Secure Shell
NTP	: Network Time Protocol
SMTP	: Simple Mail Transmission Protocol
BIND	: Berkley Internet Name Daemon
OSSTMM	: The Open Source Security Testing Methodology Manual
HTTP	: HyperText Transfer Protocol
ICMP	: Internet Control Message Protocol
DDoS	: Distributed Denial of Service
IIS	: Internet Information Service
UDP	: User Datagram Protocol

BÖLÜM I
GİRİŞ

1.1. Problem

Günümüzde kullanılan siber güvenlik çözümleri gelişmiş yöntemlerle saldırıları tespit ederek kullanıcılara ve cihazlara koruma sağlamaktadır. Birçoğu kurumsal teknolojik alt yapıları korumak için geliştirilen genellikle yüksek maliyetli ve yüksek sistem gereksinimi ihtiyacı olan ticari çözümler maliyeti artırmaktadır. Bu durum siber güvenlik anlamında gerekli yatırımların mecbur olmadıkça yapılmadığını ortaya çıkarmaktadır.

1.2. Araştırmanın Amacı

Açık kaynak kodlu yazılımlar, kodları herkese açık olarak paylaşılan, kullanıcıların yazılım üzerinde istedikleri değişiklikleri yapabildikleri ve dağıtabildikleri yazılımlardır. Donanım giderlerini, doğrudan ve dolaylı yazılım giderlerini, personel giderlerini, vs. içeren yazılımın toplam sahip olma maliyetinin düşük olması, farklı alanlar ve farklı amaçlar için kullanılabilmesindeki esneklik, yazılımın kalitesi, yenilikçi olması, ihtiyaçlar doğrultusunda geliştirilebilir olmasıdır. Bilgi güvenliği, kapalı kaynak kodlu yazılımlardan daha yüksek performans göstermesi ve daha uzun ömürlü olması gibi avantajlar kamu kurumlarının ve özel kuruluşların açık kaynak kodlu yazılımlara yönelmesini sağlamıştır.[1]

Açık kaynak kodlu yazılımların kişisel ve kurumsal kullanıcıların ihtiyaçlarına göre gelişmesi işletim sistemlerinden, bilginin güvenliği ve siber güvenliğin sağlanmasında, ofis ihtiyaçlarına kadar kullanılmaya devam etmektedir. Siber güvenlik olarak yüksek maliyetli yazılım fonksiyonlarına eş değer gelebilecek açık kaynak yazılımlar ile siber tehditleri bertaraf etme amacı güdülmektedir.

1.3. Araştırmanın Önemi

Bu çalışma ile siber tehditlerin etkilerinin artarak devam ettiği günümüzde kurumsal siber güvenlik kavramının net olarak anlaşılması, kurumsal siber güvenliğe yönelik tehditler hususunda farkındalık bilinci oluşturulması için açık kaynak yazılımlar ile siber güvenlik

yöntemleri ve siber tehdit ile ilgili model oluşturulması, siber tehditlere karşı etkin ve verimli mücadele yeteneği kazandırılması hedeflenmektedir.

1.4. Sayıltılar

Yararlanılan kaynaklar genelde açık kaynak kodlu yazılım geliştiren platformların web sitelerinden faydalanılmıştır.

1.5. Sınırlılıklar

Topolojide belirtilen sistem kurulumları sanal makine (Virtual Machine Vmware) yazılımı fiziksel tek bilgisayara kurularak yapılmıştır. Şekillerin birçoğu kurulum ve uygulama esnasında ekran (screenshot) çıktısı alınarak ve açık kaynak platform geliştiricilerinden kaynak gösterilerek bu çalışmaya eklenmiştir. Saldırılarda tanımlanan alarm rolleri toplu olarak da girilebildiği gibi bu çalışmada saldırı türüne göre alarm rolü girilmiştir.

1.6. Tanımlar

1.6.1.Vmware Sanallaştırma Yazılımı

Fiziksel Bilgisayar üzerine sanal olarak birden çok işletim sistemi kurmamızı sağlayan, bunu sağlarken de bilgisayarımızın donanımını kullanan ve fiziksel bilgisayar ile sanal makine arasında bir köprü vazifesi görür. Sanal sunucu pazarında Vmware ihtiyaca göre Vmplayer, Vmware Workstation ve Vmware Vspare ürünlerini, Oracle firmasının geliştirdiği VirtualBox, Microsoft firmasının Virtual PC gibi ürünler geliştirilmektedir.

Sanallaştırmada en çok tercih edilen ve bu konuda en tecrübeli yazılımlardan birisi olan Vmware ücretli ve ücretsiz kullanım için farklı sürümler ile hizmet sunmaktadır. Bu hizmetlerde devamlılık, yedekleme ve bakım işlemlerinin kolay yapılmasından kaynaklı olarak sektörde birleşik uç nokta yönetim araçları konusunda öncü konumdadır. [2]

Bu çalışma içerisinde ağ teknolojileri konusunda esneklik sağlayan Vmware Workstation yazılımı kullanılmış olup, ilgili ağ topolojisinin oluşturulması ve gerçeklenmesi sağlanmıştır.

1.6.2. İşletim Sistemleri

Bu çalışmada yer alan uygulamaların üzerinde çalışacağı işletim sistemlerinden bahsedilmiştir.

1.6.2.1. FreeBSD

FreeBSD, özelliklere, hıza ve kararlılığa odaklanan çeşitli platformlar için bir işletim sistemidir. Berkeley, California Üniversitesi'nde geliştirilen UNIX sürümü BSD'den türetilmiştir.Büyük bir topluluk tarafından geliştirilir ve korunur. Temel amacı kararlılık ve güvenlik olan bir UNIX çeşidi olmakla birlikte FreeBSD, bir güvenlik duvarı için gerekli tüm şartları standartlara uygun, sağlam ve esnek bir yapıda sunar. İşletim sistemi, temelini oluşturan proaktif güvenlik politikası ile bilinen birçok güvenlik zafiyetine karşı korunduğu gibi geliştirdiği alternatif çözüm önerileri ile gelecekte çıkabilecek birçok problemi temelden çözmüştür. Bu çalışmada Pfsense güvenlik duvarı dağıtımı ile birlikte kullanılmıştır.[3]

1.6.2.2. Kali Linux

Kali Linux; Linux Debian Kernel (çekirdek) tabanlı 2013 yılında BackTrack Linux'un yeniden yapılandırılması ile oluşturulmuş genel anlamda güvenlik kontrol ve sızma testlerinin yapılması için Offensive Security Co. Aracılığıyla Devon Kearns, Mati Aharoni ve Raphael Hertzog tarafından geliştirilip, dağıtımı kalilinux.org web adresi üzerinden yapılmaktadır. Sistem ile gelen network ve diğer araçlar sayesinde birçok alanda (ağ, Windows, Arduino) güvenlik testi yapmak ve yazılım geliştirmek mümkündür. Masaüstü ortamı olarak KDE GUI kullanmamakla birlikte, GNOME ve XFCE ortamını kullanmaktadır. 64-bit (amd64), 32bit (i386), ARM ve Armel işlemci altyapısı desteği sunmaktadır. [4]

1.6.2.3. Microsoft Windows

Microsoft Windows, kullanıcıya grafik arabirimler ve görsel iletilerle yaklaşarak, yazılımları çalıştırmak, komut vermek gibi klavyeden yazma zorunluluğunu ortadan kaldıran, Microsoft şirketinin geliştirdiği dünyada en çok kullanılan bir işletim sistemi ailesidir. [5]

Windows, Windows 10, Windows 7'nin yüzde 36,90'lık pazar payını geride bırakarak yüzde 39,22 pazar payıyla masaüstü işletim sistemlerinde liderliği ele geçirdi. İki

işletim sistemi, toplamda yüzde 76,12'lik payla sektöre liderlik ediyor. Yani 10 bilgisayardan yaklaşık 8 tanesi Windows 10 veya Windows 7 kullanıyor. [6]

Windows Vista'dan sonra Microsoft, Windows 7 ile başarıyı yakalamış bu başarıyı Windows 8 ile devam ettirmektedir. Microsoft Windows ailesinin son üyesi 1 Ekim 2014'te piyasaya çıkan Windows 10'dur. [7]

1.6.3. PfSense

Pfsense projesi, özel çekirdeğe sahip FreeBSD işletim sistemine dayanan ve ek işlevsellik için üçüncü taraf ücretsiz yazılım paketleri içeren ücretsiz bir ağ güvenlik duvarı dağıtımıdır. Pfsense yazılımı, paket sisteminin yardımıyla, yapay sınırlamalar olmaksızın aynı işlevselliği veya daha fazla yaygın ticari güvenlik duvarını sağlayabilir. Bazı durumlarda, Pfsense ticari kapalı kaynak çözümlerinde bulunmayan ek özellikler içerir.[8]

Pfsense yazılımı, dâhil edilen tüm bileşenlerin yapılandırılması için bir web ara yüzü içerir. Herhangi bir UNIX bilgisine, komut satırını herhangi bir şey için kullanmaya ve kural kümelerini manuel olarak düzenlemeye gerek yoktur. Ticari güvenlik duvarlarına aşina olan kullanıcılar web ara yüzünü hızlı bir şekilde öğrenir, ancak ticari sınıf güvenlik duvarlarına aşina olmayan kullanıcılar için bir öğrenilmesi zaman almaktadır.

Bu çalışma içerisinde güvenlik duvarı rolündeki sunucu sistemde kurulup, uygulama olarak kullanılmıştır.

1.6.4. Snort

Snort açık kaynak kodlu saldırı tespit ve engelleme sistemi yazılımıdır. Cisco (SourceFire) tarafından 1998 yılından beridir geliştirilmektedir. Yaygın olarak kullanılan saldırı tespit sistemlerinden biridir. Genel olarak imza tabanlı olarak çalışan Snort, protokol ve anomali analizi yapabilme yeteneğine de sahiptir. Kullanıcıların kendi kurallarını yazmasına imkân sağlayacak esnek bir kural diline sahiptir. Ücretsiz ve açık kaynak kodlu olması, özellikle araştırma amaçlı yaygın olarak kullanılmasını sağlamaktadır. Açık kaynak dünyasının gücünü de arkasına alan Snort sürekli gelişen bir uygulamadır.[9]

Snort, bu çalışma içerisinde tehdit gözetleme sistemi yazılımı olarak kullanılmıştır.

BÖLÜM II
SALDIRI TESPİT SİSTEMLERİ

2.1. Bilgi Güvenliği

Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır ve "gizlilik", "bütünlük" ve "süreklilik(erişilebilirlik)" olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik zafiyeti oluşur. [10]

Gizlilik (Confidentiality), bilginin yetkisiz kişilerce erişilememesidir. Bütünlük (Integrity), bilginin doğruluğunun ve tamlılığının sağlanmasıdır. Bilginin içeriğinin değiştirilmemiş ve hiçbir bölümünün silinmemiş ya da yok edilmemiş olmasıdır. Erişilebilirlik (Availability), bilginin bilgiye erişim yetkisi olanlar tarafından istenildiği anda ulaşılabilir, kullanılabilir olmasıdır. [11]

Bilgi Güvenliği Yönetimi, kasıtlı/kasıtsız bilişim sisteminde bulunan çeşitli varlıkların sebep olduğu gizlilik, bütünlük ve erişilebilirlik ihlalleri için koruyucu, önleyici, düzeltici ve iyileştirici faaliyetlerin bütünüdür.

Bilgi Güvenliği Yönetimi sayesinde kuruluşun iş sürekliliğine katkıda bulunulması, kuruluş imajının bilgi güvenliği ihlali sebebi ile zedelenmesinin önlenmesi, bilgi güvenliği ihlali gerçekleşmesi halinde uygun yönetimin sağlanarak oluşabilecek zararı minimumda tutacak gerekli planların uygulanması sağlanabilecektir. Bu da kurum ve kuruluşlar için bilgi güvenliğinin sağlanmasının ne kadar önemli olduğunu belirtmektedir.

2.2. Siber Güvenlik

Siber güvenlik, elektronik ortamda gerçekleşen işlemler sırasında varlıkların bilinçsizliğinin sebep olduğu hatalardan veya kötü niyetli kişilerin saldırılarından kaynaklanan eylemler sonucunda zarar görmesini engellemek amacıyla alınan tedbirler şeklinde tanımlanır.

Siber güvenlik kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, elektronik haberleşme sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır. Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır (www.btk.gov.tr).

2.2. Saldırı Tespit Sistemleri

Bilişim alanında tehdit sayılarının ve türlerinin hızla artmasıyla birlikte, saldırı tespit ve güvenlik teknolojilerinde hızlı bir gelişim ve değişim yaşanmaktadır. Sistemlerin güvenliğini sağlamak, bilgiyi yetkili olmayan kişilerin ele geçirmelerini engellemek için kimlik doğrulama algoritmalarından, erişim kontrolü gibi savunma mekanizmaları geliştirilmiştir. Güvenliğin ilk basamaklarından biri olan bu tip mekanizmalar internetin yaygınlaşması ile birlikte bilgi sistemlerine olan ciddi artış ve saldırıların tiplerinde de yeni alanlar oluşturmaktadır. Saldırı tespit sistemleri, tüm tedbirlere karşın bilgisayar sistemlerine yapılan saldırıları gerçekleşirken ya da gerçekleştikten sonra tespit etmek, İnternet 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. Saldırı tespit sistemleri bir nevi alarm sistemi olarak düşünülebilir. [12]

Saldırı tespit sistemleri, internet ağının gelişimi ve saldırı türlerinin her geçen gün değişim ve metotlarının gelişiminde uzmanlık alanlarına göre sınıflandırılmıştır. Bunların bazıları;

- Ağ Saldırı Tespitleri

- Kötüye Kullanım Tespitleri
- Anormallik Tespit Sistemleri
- Kullanıcı Tabanlı Saldırı Tespit Sistemleri
- Stack Tabanlı Saldırı Tespit Sistemleri

2.3. Açık Kaynak Kodlu Siber Güvenlik Yazılımları

Yazılım dünyasında epey süredir var olan popülaritesi her geçen gün artan Açık Kaynak Kodlu yazılımlar herkes tarafından erişilebilen kaynak kodları sayesinde kolaylıkla erişilebilen, üzerinde değişiklik yapılan ve değişiklikleri paylaşmayı zorunlu kılmayan yazılım geliştirme metodolojisidir.

Açık Kaynak kodlu yazılımların Türkiye'de uygulaması ile ilgili yapılan çalışmalarda önemli bir ivme elde edilmiştir.[10] Kamu alanında yapılan bu çalışmada açık kaynak kodlu yazılımların güvenli olması, toplam tedarik etme maliyetleri ve diğer etkenler ile bir adım önde olduğu belirtilmektedir.

2.4. Ağ Topolojisinin Oluşturulması

Ağ Topolojisi oluşturulmasında kullanılan gerekli donanım özellikleri ve yazılımların sürüm numaraları Tablo 1.1 ve Tablo 1.2 de gösterilmiştir.

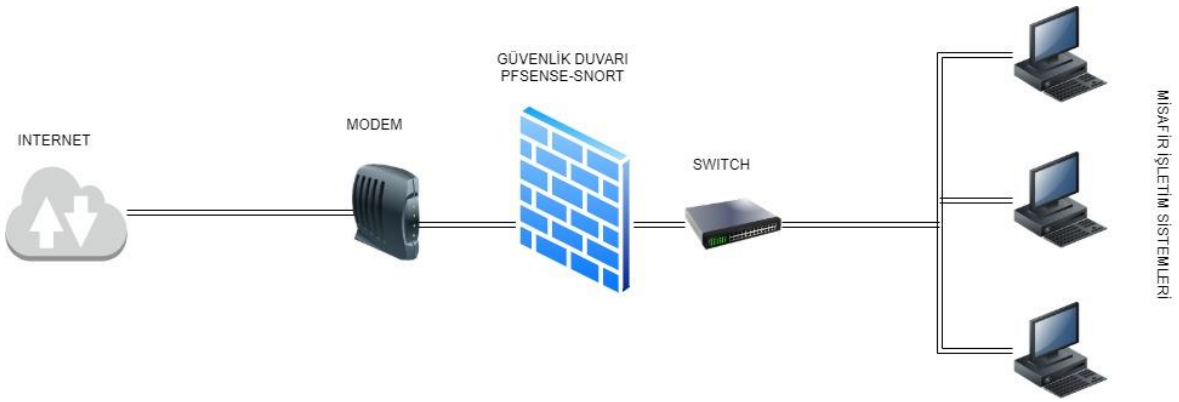
İşlemci	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 1800 Mhz, 4 Çekirdek, 8 Mantıksal İşlemci
Bellek	8 GB DDR4

Tablo 1.1. Donanım Özellikleri

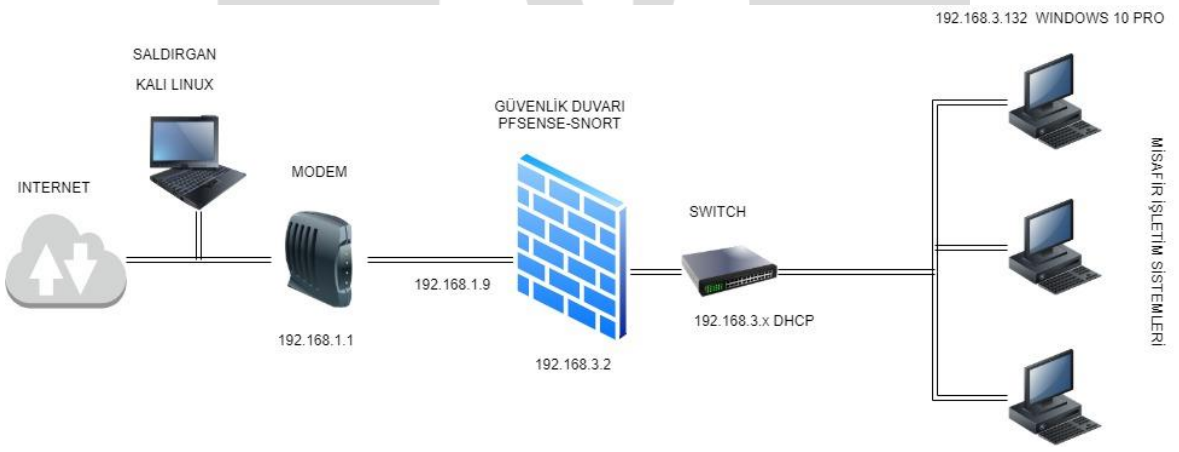
Sunucu İşletim Sistemi	Windows 10 Enterprise
Güvenlik Duvarı İşletim Sistemi	FreeBSD Pfsense 2.4.5, Snort 2.4.5
Misafir İşletim Sistemi	Windows 10 Pro
Saldırgan İşletim Sistemi	Kali Linux 2020.2

Tablo 1.2. Kullanılan Yazılım ve Sürüm Numaraları

Projede uygulanacak olan temel topoloji şeması Şekil 1. de belirtilmiştir. Çalışma içerisin de kullanılacak olan topoloji içerisinde yer alan sistemlere ait ip adres bilgisi ve rolleri Şekil 2.2'de gösterilen topolojideki gibi olmaktadır.



Şekil 2.1. Temel Topoloji Şeması Genel Konumlar

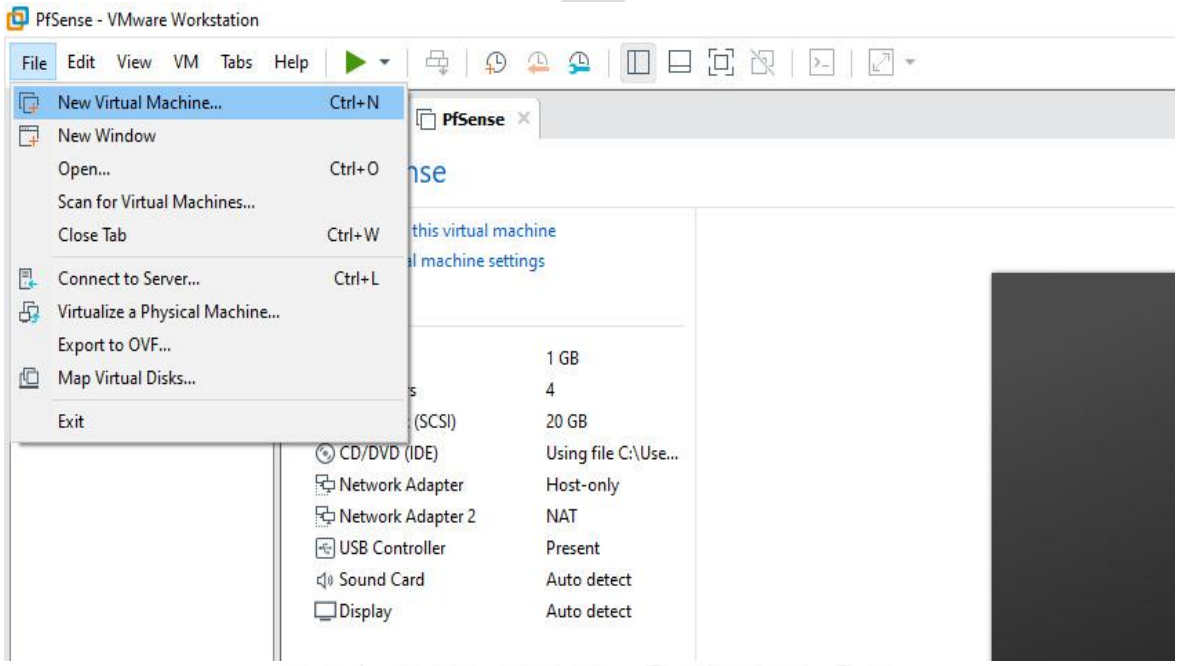


Şekil 2.2. Genel Ağ Topolojisi Saldırgan Konumu

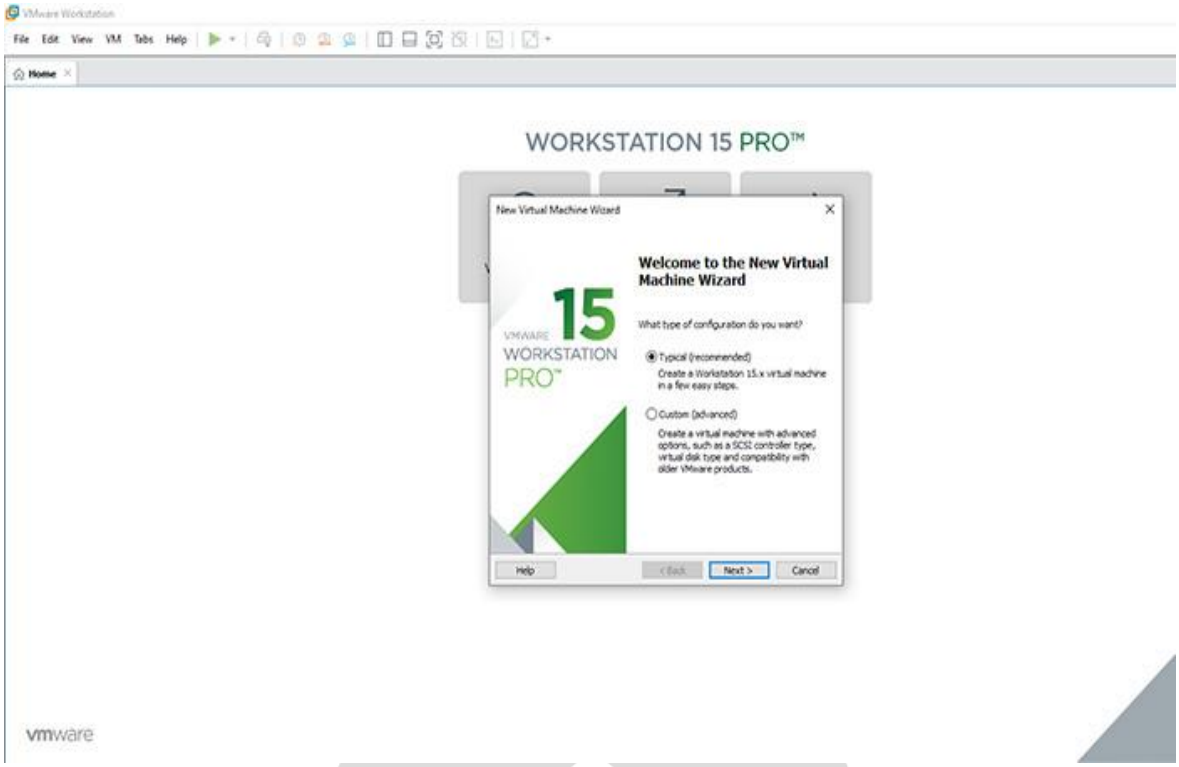
2.5. Vmware Kurulumu ve Yapılandırılması

2.5.1. Sanal Makina Oluşturulması

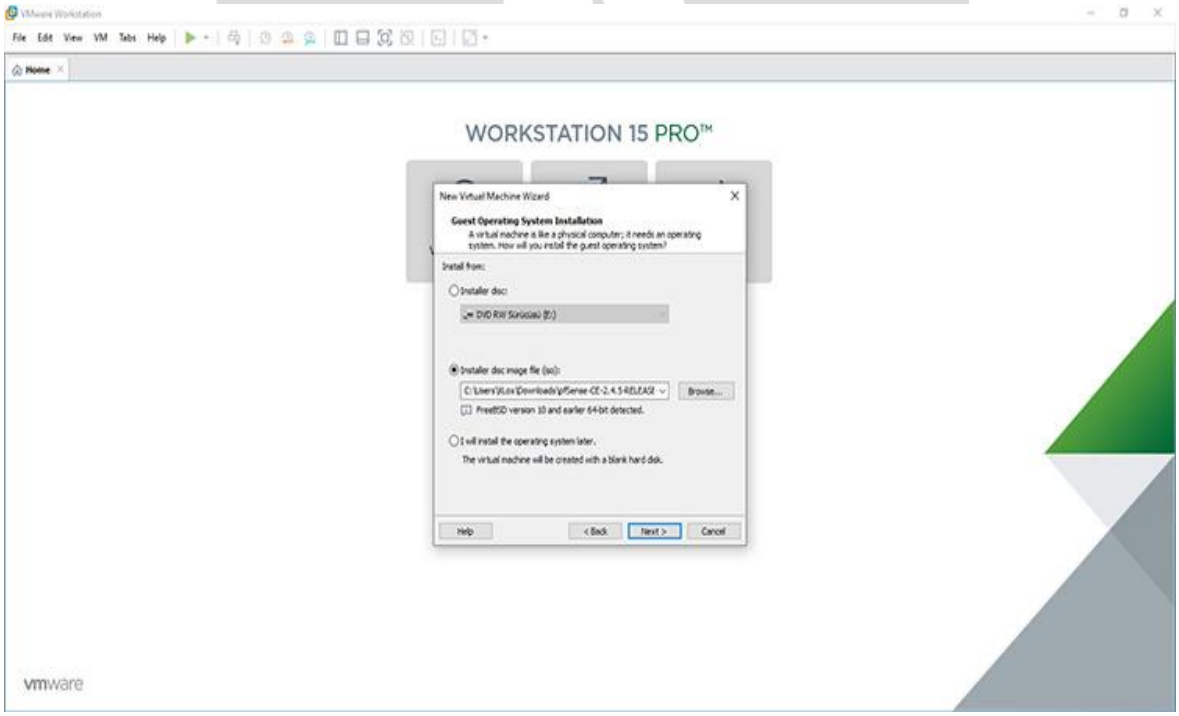
Vmware Workstation sanallaştırma yazılımında temel olarak aşağıda belirtilen şekilde sanal makinalar oluşturulacaktır. Uygulama yazılımlarının donanım ihtiyacına göre Vmware kaynaklarında değişiklik yapılabilir. Ağ ayarları yapılanması için Pfsense iki adet network kartına ihtiyaç duyar. Wan ara yüzü sayesinde iç ağda bulunan uçların internete çıkar. Lan ara yüzü ise firewall/ router görevlerinin yeri getirmesi ve uçların yönetilmesi için kullanılır.



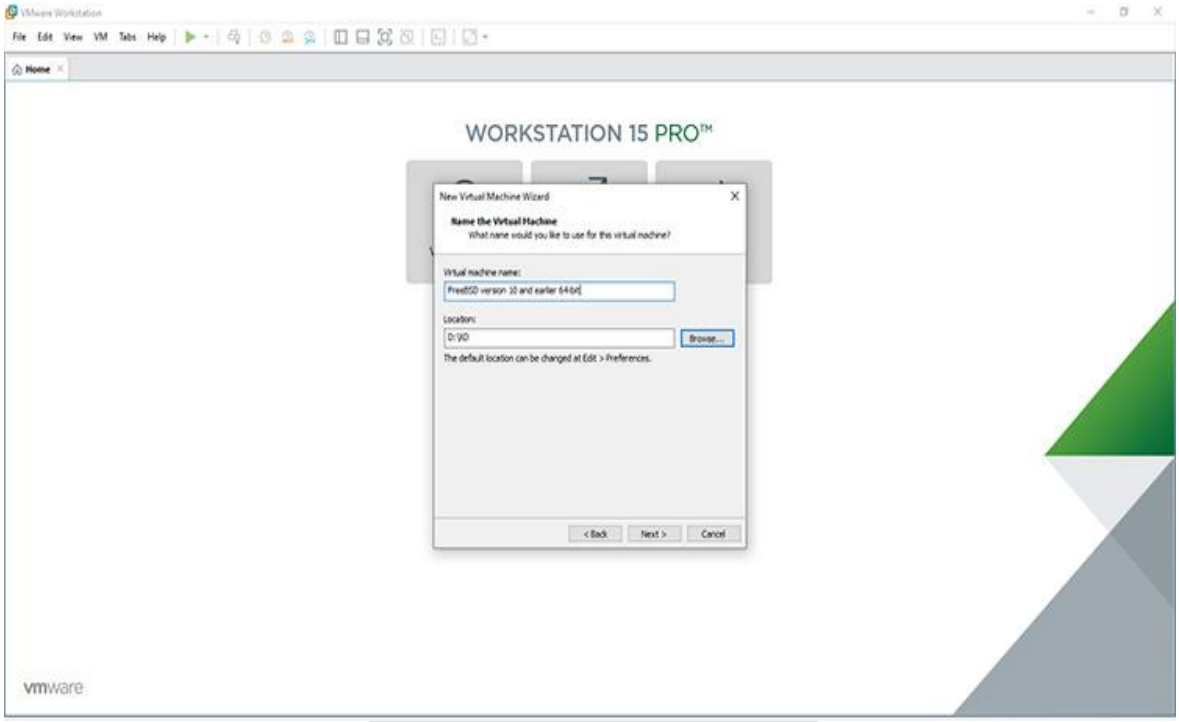
Şekil 2.3. Yeni Sanal Makine Oluştur Seçimi



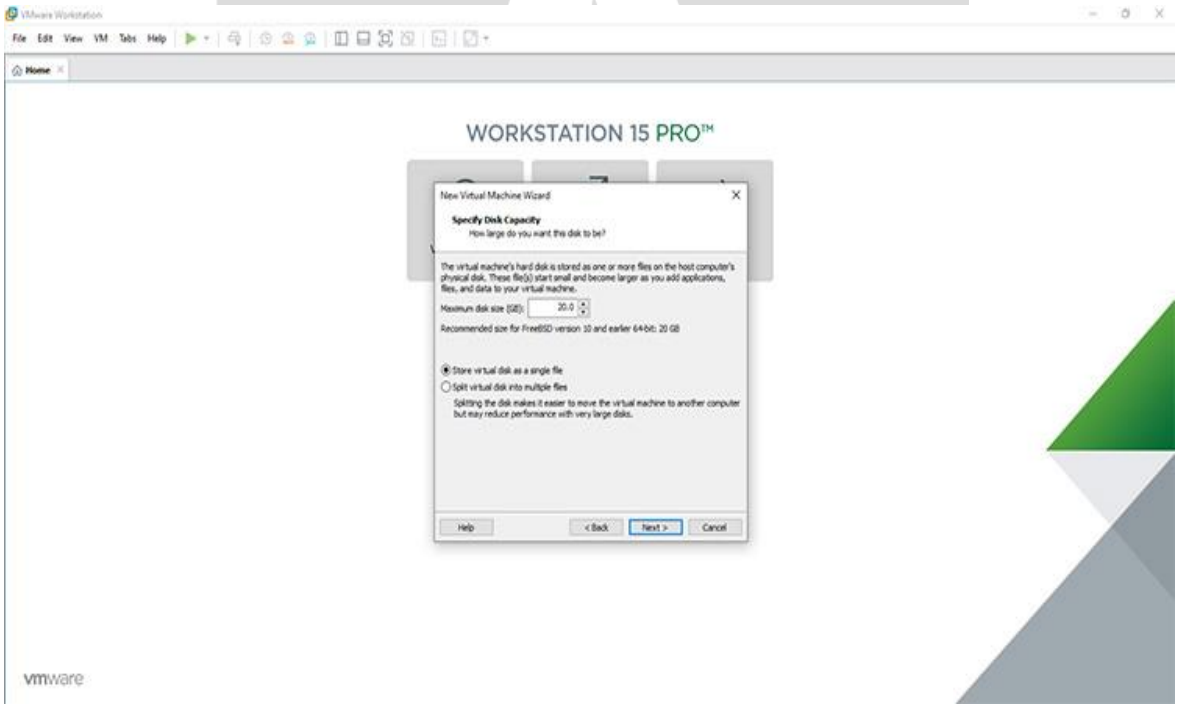
Şekil 2.4. Tipik Seçim



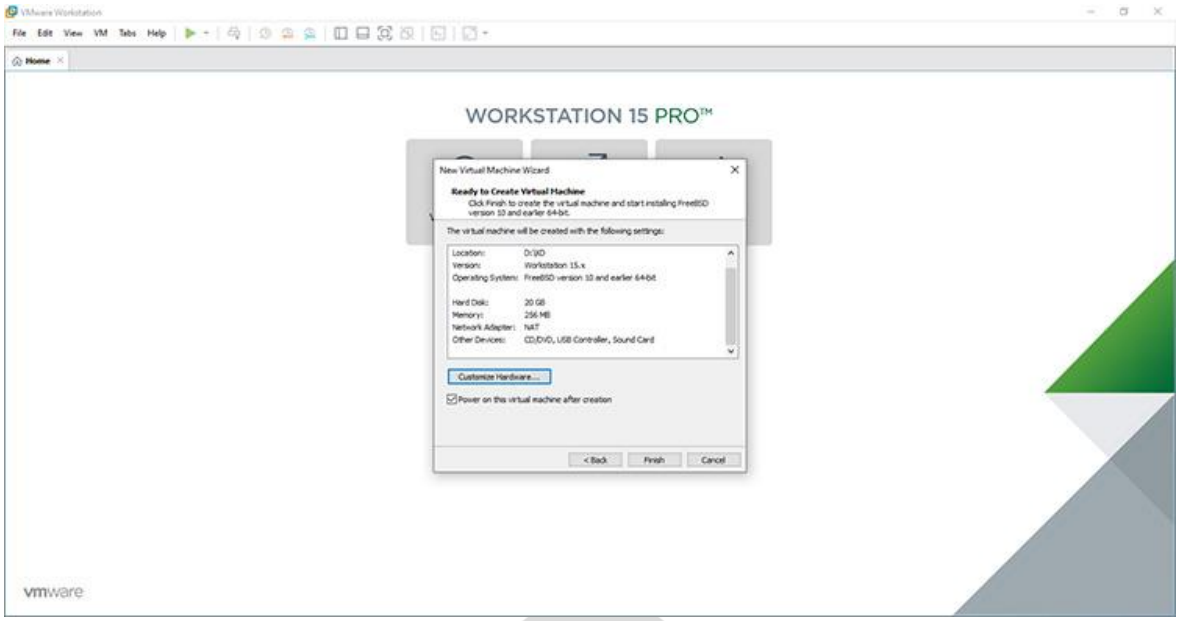
Şekil 2.5. Kurulacak sistemin ISO dosyasının seçimi



Şekil 2.6. Kurulacak olan işletim sisteminin konumu ve sanal dosya adının belirlenmesi



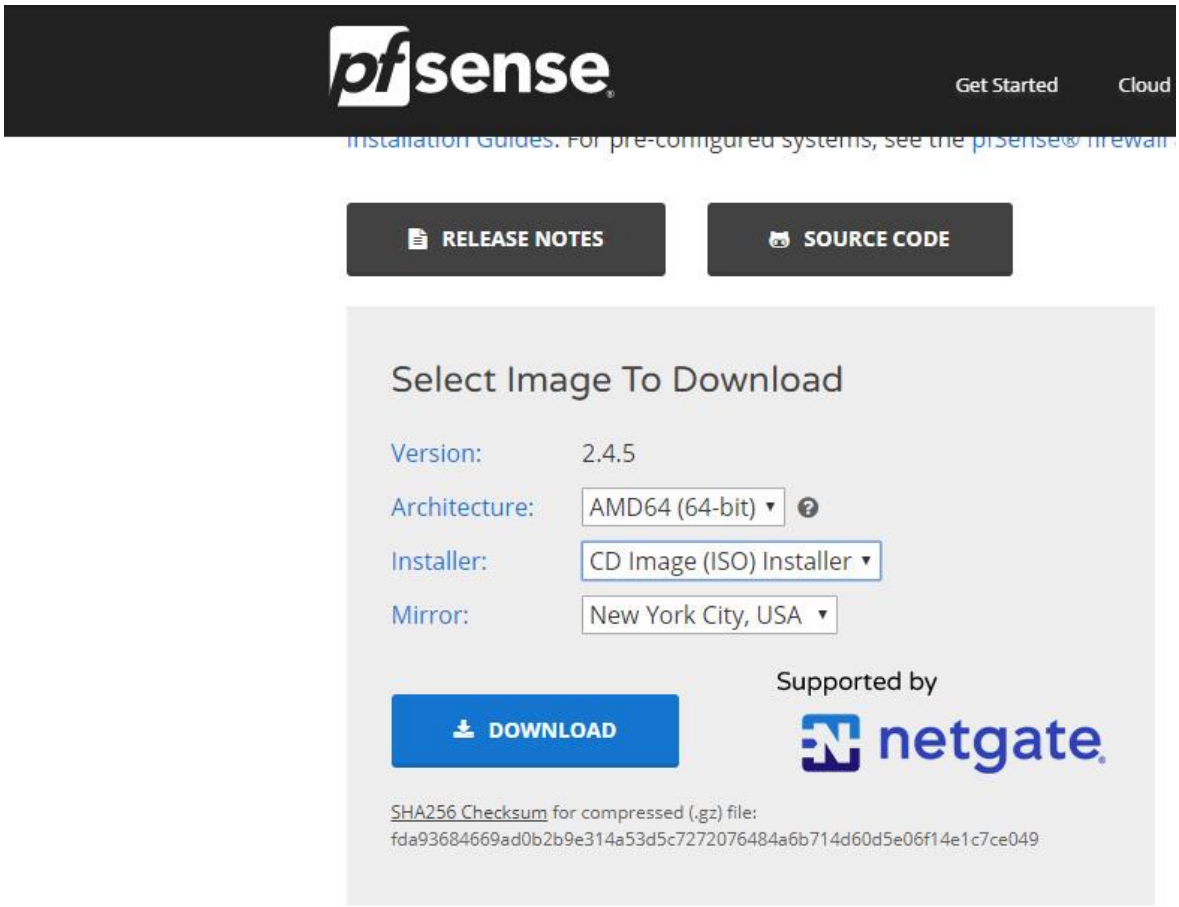
Şekil 2.7. Kurulacak sistemin sanal üzerinde kapasitesinin belirlenmesi



Şekil 2.8. Sanal Sistem Konfigürasyonu Listesi

2.6. Güvenlik Duvarı Pfsense Kurulumu ve Yapılandırılması

Pfsense kurulumu için https://www.Pfsense.org/download/ adresinden resimde görüldüğü üzere ISO uzantılı dosyasını indirilmektedir.



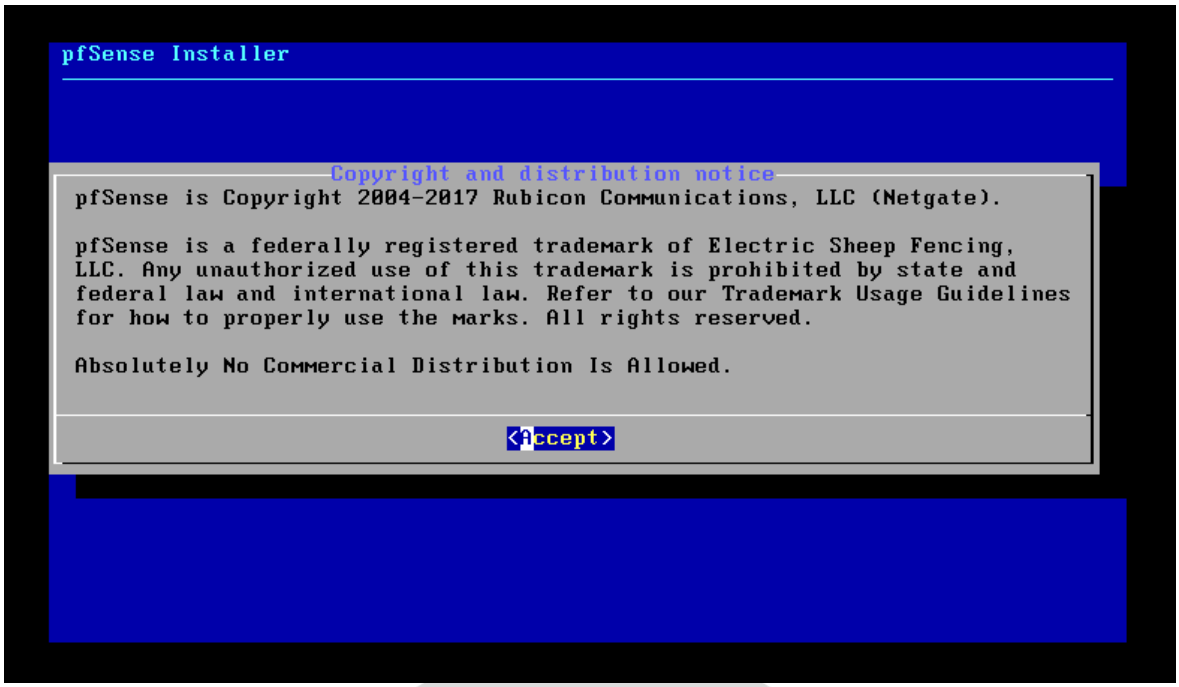
Şekil 2.9. Pfsense ISO dosyası indirme

Sanal makine için aşağıda belirtilen kaynaklardan yararlanılarak sanal makina oluşturulmuştur.

İşlemci	2 Core
Bellek	1 GB
Kapasite	30 GB
Network	Lan ve Wan Bacağı için 2 adet Network Adaptör

Tablo 2.3. Pfsense için Sanal Makine Özellikleri

Sanal makine kurulumunu yukarıda belirtilen şekillerde yapılmıştır. Güvenlik duvarı kurulumu aşağıda adım adım anlatılmaktadır.



Şekil 2.10. Pfsense Telif Hakları

Sanal makinede Pfsense güvenlik duvarını başlattığımız anda ilk karşımıza çıkan ekran telif hakları ve dağıtım bildirimidir. Kabul edilerek devam edilir.

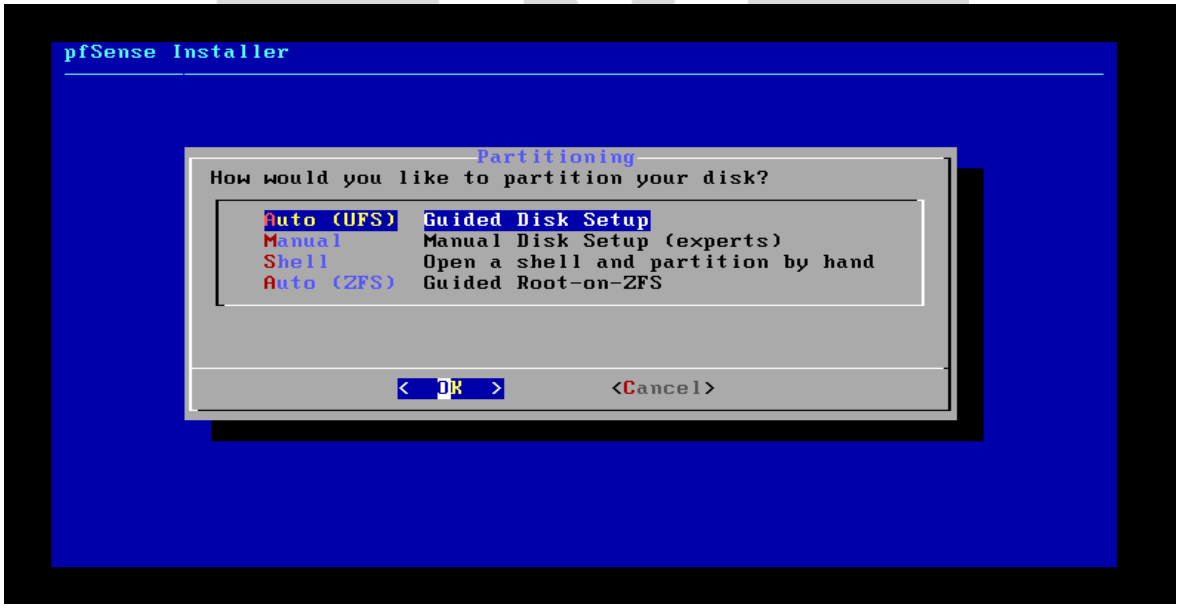
Şekil 2.11. Pfsense Hoş Geldiniz Ekranı

Hoş geldiniz ekranında 3 seçenek bulunmaktadır. 1.seçenekte Pfsense kurulumunu başlatmak için kullanılır, 2.seçenekte daha önce kurulumu yapılan Pfsense için bize bir

kurtarma kabuğu çalıştırır ve 3.seçenekte Pfsense önceden yüklü ise Pfsense yapılandırma ayarları bulunan dosyayı kurtarmamızı sağlamaktadır.

Şekil 2.12. Keymap seçenekleri

Kullanacağımız klavye tipi seçildikten sonra devam edilir.



Şekil 2.13. Disk Bölümleme

Pfsense'yi kuracağımız diski bölümlendirmek için, ilk seçenekte otomatik olarak tüm diski kullanarak UFS dosya sisteminde kurulumu başlatır, 2.seçenekte diski manuel olarak elle bölümleyebilir, 3.şeçenekte de bir kabuk çalıştırır ve el ile bölümleme yapabilirsiniz ve 4. son seçenekte yine otomatik olarak ZFS dosya sisteminde kurulumu başlatabilirsiniz.

Şekil 2.14. Pfsense Kurulum

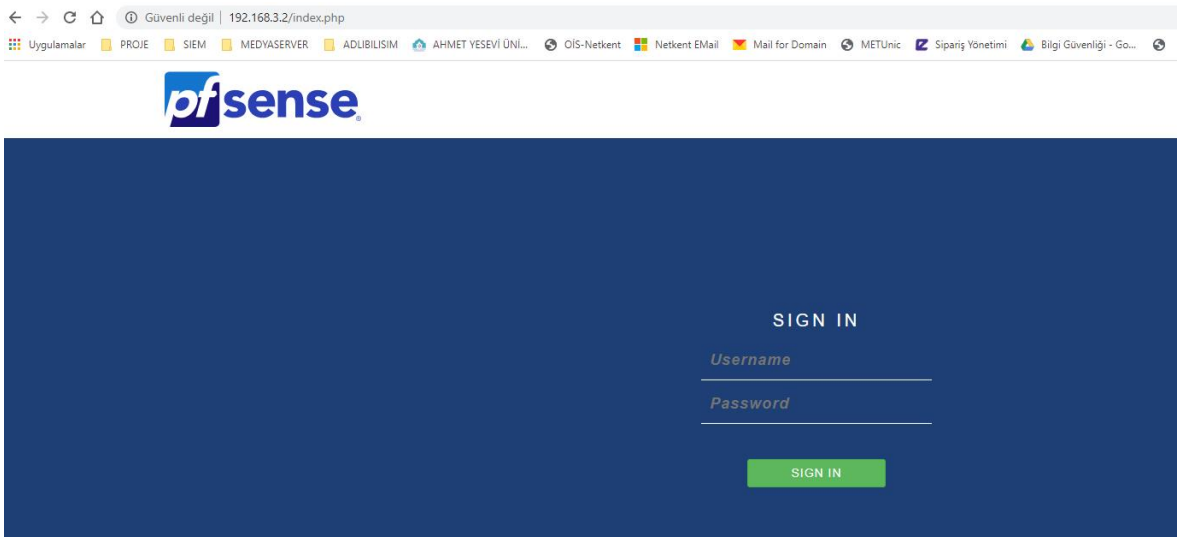
Bu adımda ise gerekli dosyalar ayarlanıp kuruluma devam etmektedir.

Şekil 2.15. Manuel Yapılandırma Sorgulama Ekranı

Manuel yapılandırmayı ekrandaki gibi seçerek yapabiliriz. Yapılandırma için bu adımda “No” seçip, sonraki seçenekte sistemi “Reboot” ederek yeniden başlatıyoruz. Pfsense IP adres yapılandırması için sistem yeniden başladığında aşağıda belirtilen seçenekler gelmektedir.

Şekil 2.16. Pfsense Başlangıç ve Yapılandırma Seçenekleri

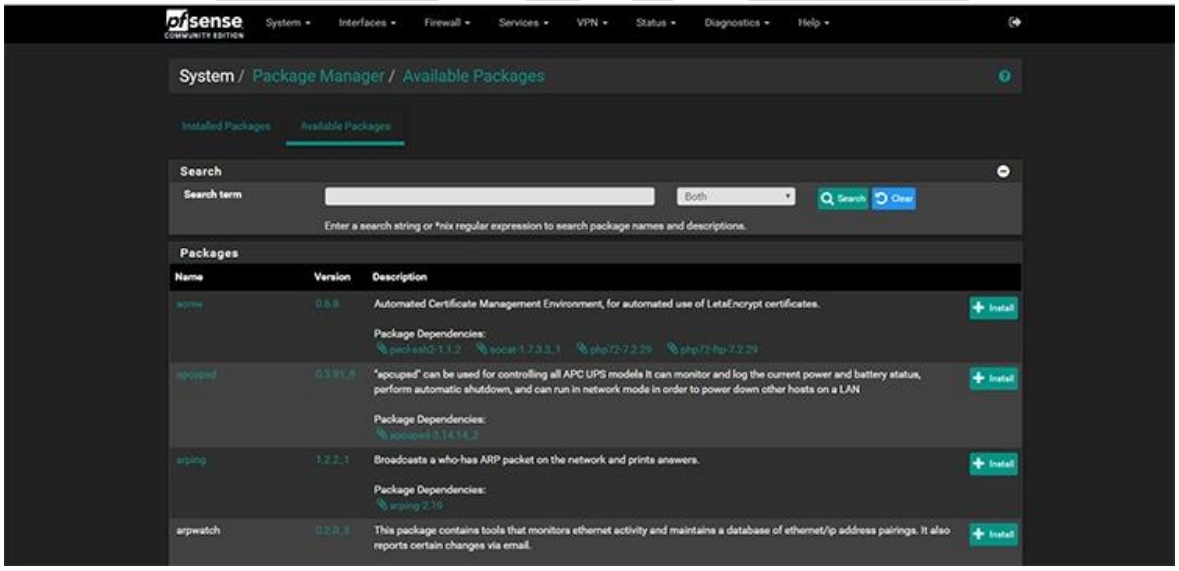
Makinemizi açtığımızda karşımıza yapılandırma ekranında LAN ve WAN IP adreslerini değiştirmek için 2.seçenek olan “Set interface IP adress” seçeneğini seçerek değiştirebiliriz. LAN ve WAN IP adresleri default olarak otomatik verilmektedir. Söz konusu yapılandırma Şekil 16. daki gibi yapılmıştır. Yapılandırma tamamlandıktan sonra Pfsense Web ara yüzüne 192.168.3.2 adresinden erişebiliriz. Pfsense default olarak kullanıcı adını “admin” ve şifre olarak da “Pfsense” olarak belirlemektedir.



Şekil 2.17. Pfsense Erişim Ekranı

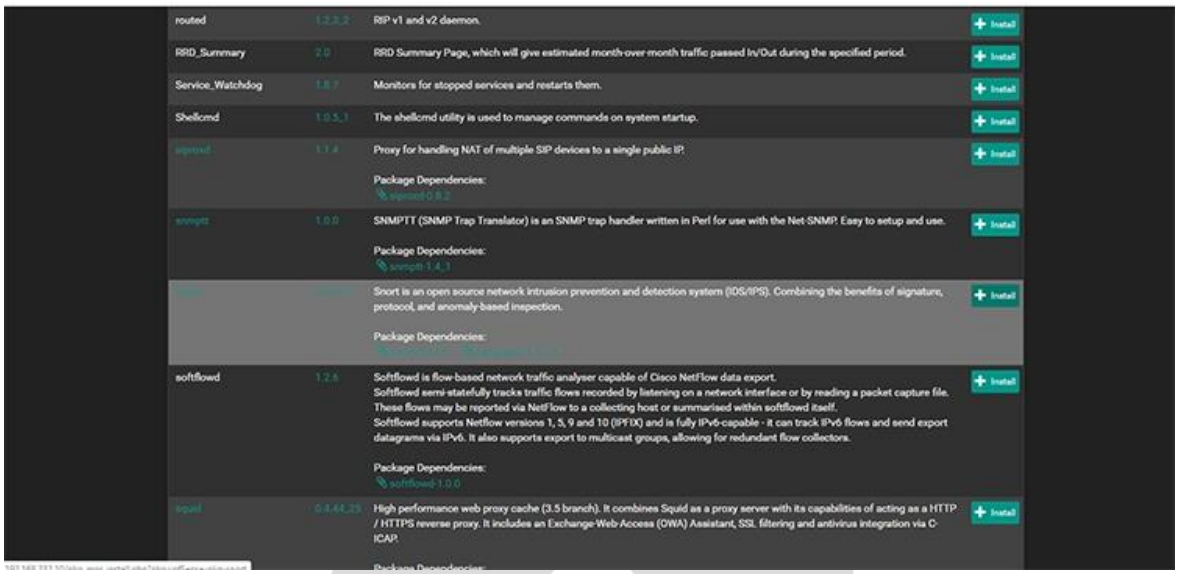
2.7. Snort Kurulumu ve Yapılandırılması

Pfsense kurulumu yapıldıktan sonra Pfsense web arayüzünden Snort paketini kurulumu yapılır. Bunun için “System / Package Manager / Available Package” kısmına geçilir. Şekil 18.

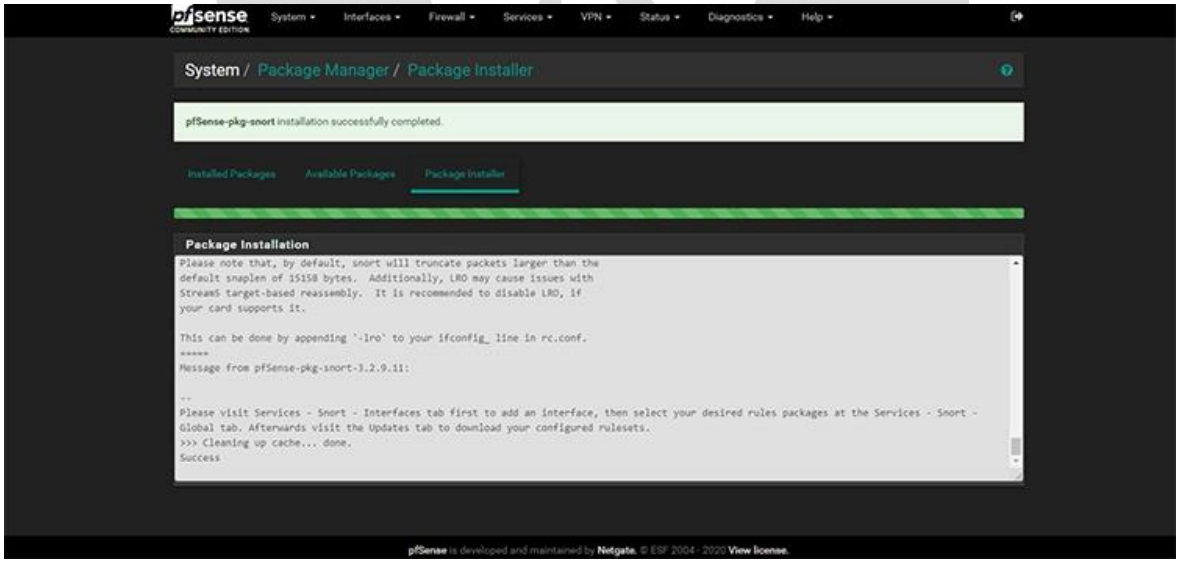


Şekil 2.18. Pfsense mevcut paketler bölümü

Paket kurulumunu sırasıyla “Available Package” bölümünden gelen listede Snort’u bulunur ve install (kur) ile paket çevrimiçi olarak indirilip kurulum gerçekleşir. Şekil 2.19. ve Şekil 2.20.

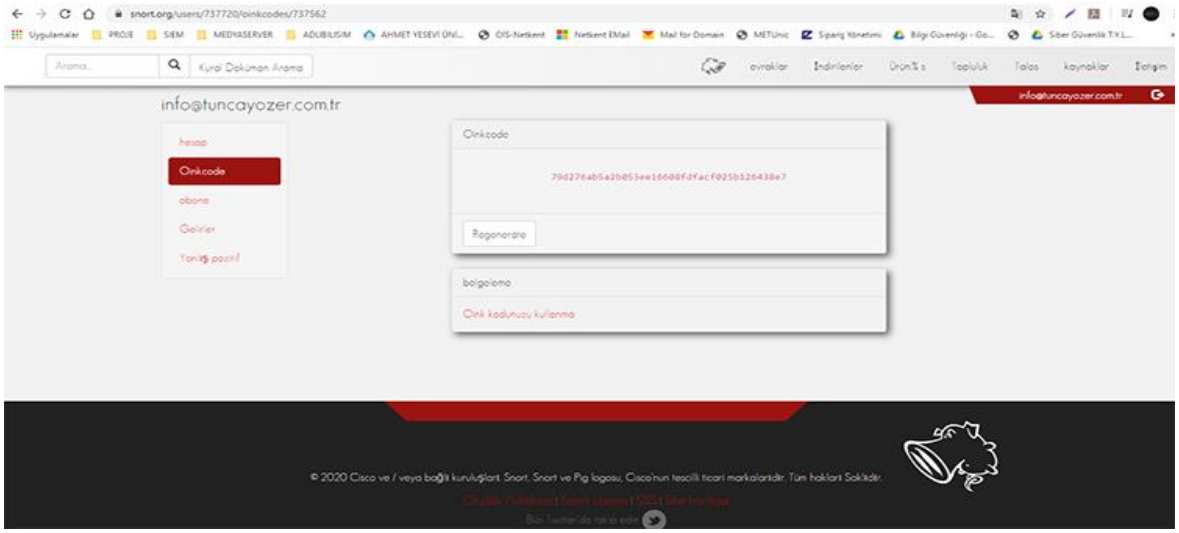


Şekil 2.19. Paketler Listesi



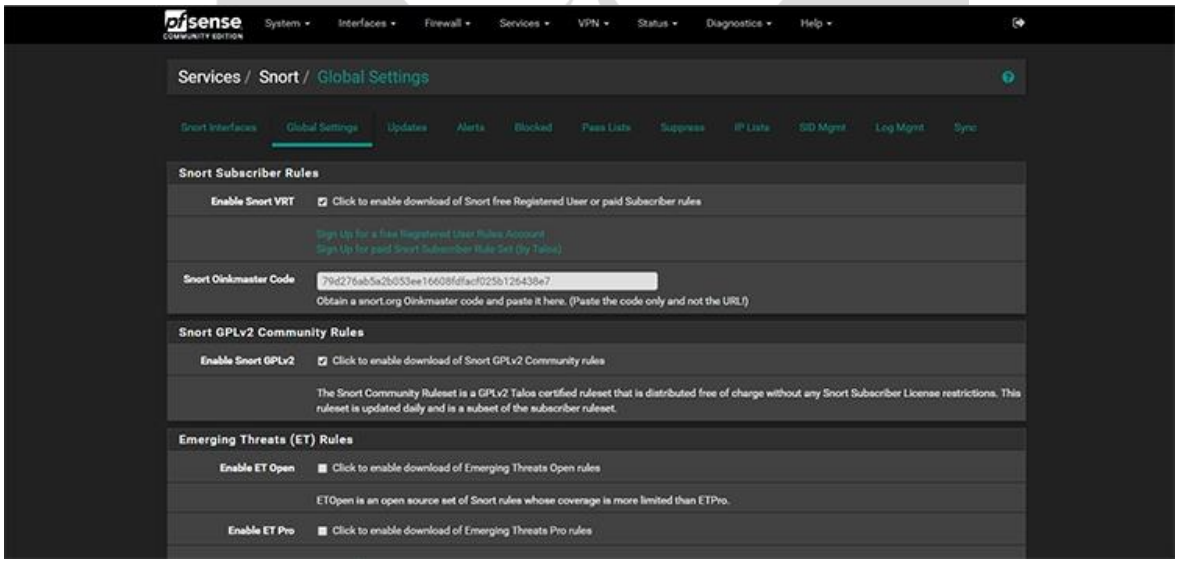
Şekil 2.20. Snort Kurulumu

Snort yapılandırmamızda snort veritabanını internet üzerinden sürekli olarak güncellememize olanak tanıyan https://www.snort.org/ adresine bir üyelik hesabı oluşturulur ve bir oinkcode alınır. Şekil 21.



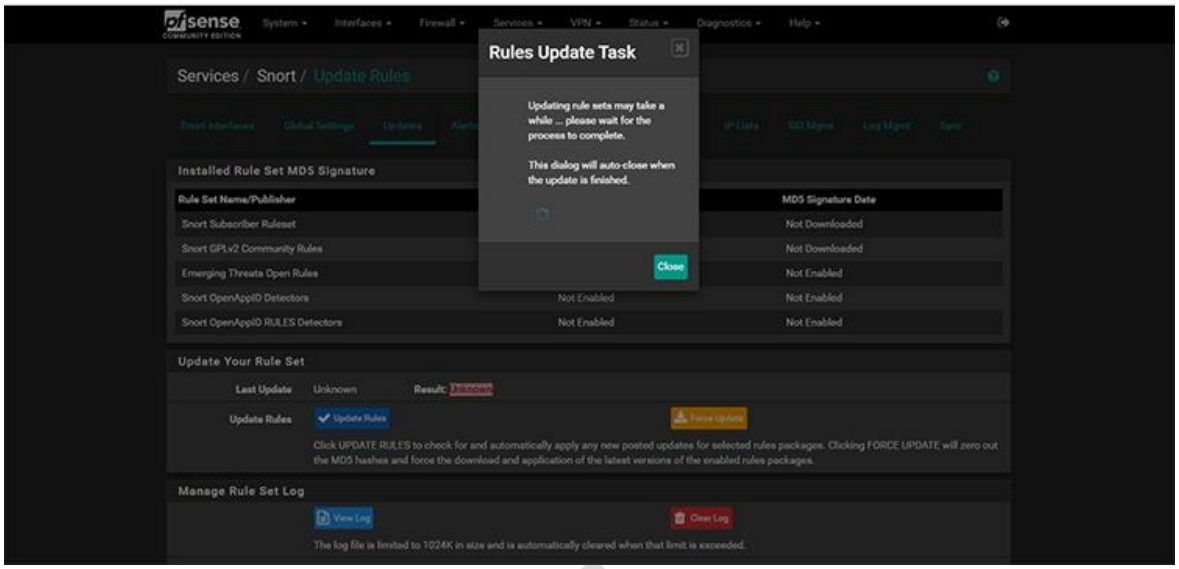
Şekil 2.21. Snort OinkCode ekranı

Pfsense web ara yüzünde Genel Ayarlar (Global Settings) sekmesine gelinir, install snort VRT Rules kutucuğunu işaretlenir ve siteden alınan oinkcode kodu Şekil 22. de görüldüğü üzere yazıp alt kısımda Save (kayıt) işlemi yapılır.

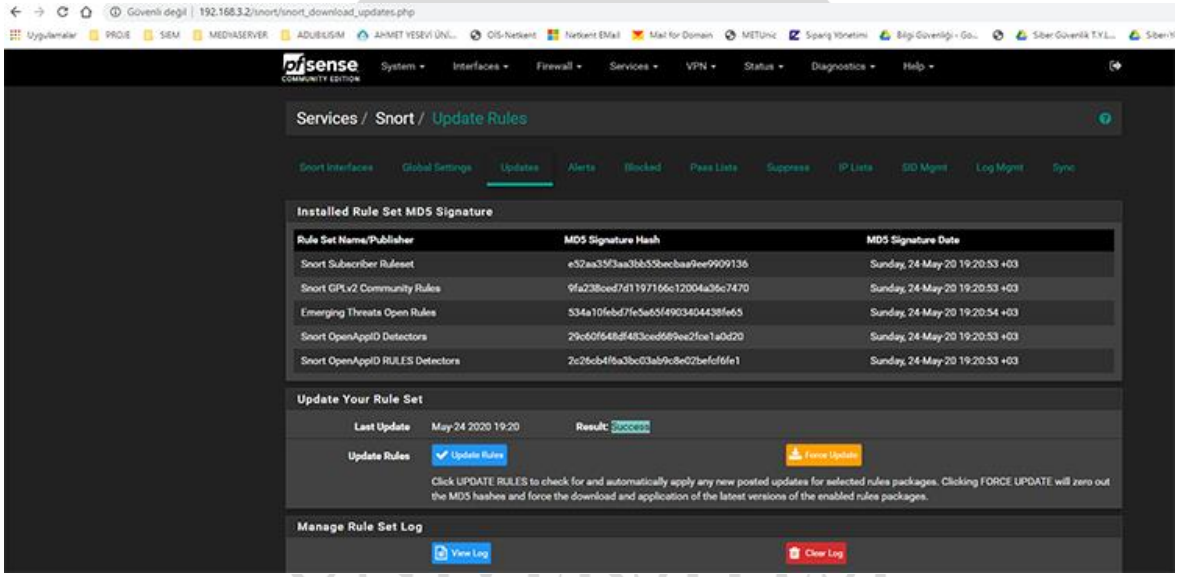


Şekil 2.22. Snort Oinkcode Giriş Ekranı

Sırada Update kısmında yeni kurmuş olduğumuz Snort rules (rolleri) ‘ları internet üzerinden canlı olarak güncelleme (update) yapıp kurulum için işlemi bitirilir. Şekil 23 ve Şekil 24.



Şekil 2.23. Snort Rule Update İşlemi



Şekil 2.24. Snort Rule Update İşleminin Bitimi

2.8. Misafir İşletim Sistemlerinin Kurulması

Ağ topolojisinin oluşturulmasında kullanılacak olan aynı zamanda Vmware Workstation uygulaması içerisinde kurulum adımları gerçekleştirilecek olan misafir işletim sistemleridir. Saldırgan Sanal Makine de Kali Linux, Kurban Sanal Makine de Windows 10 Pro işletim sistemi kullanılmıştır. Sanal makine özellikleri;

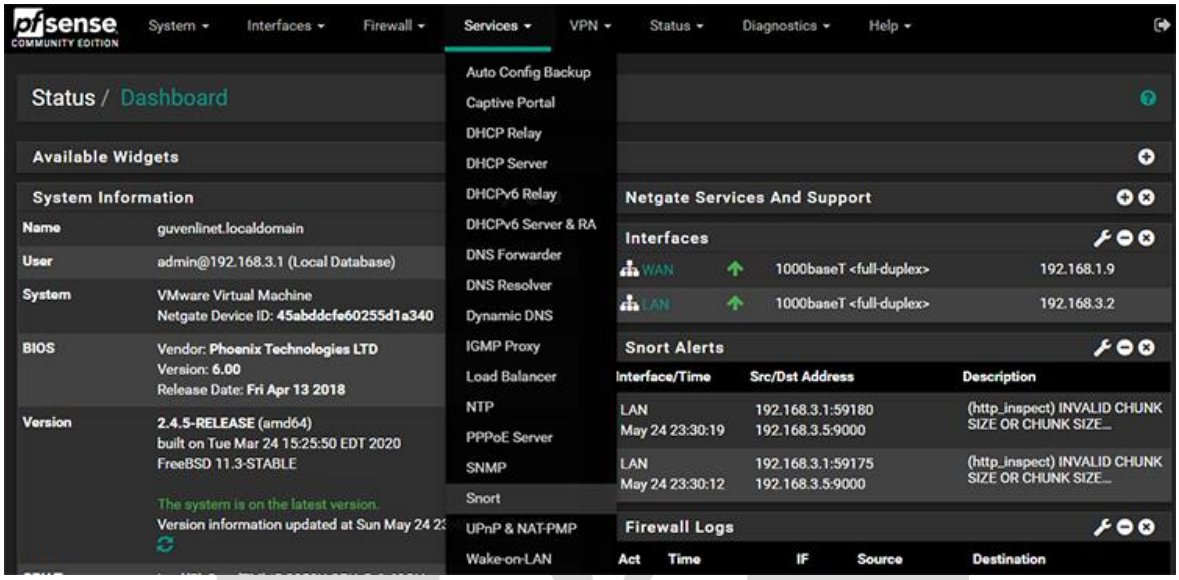
İşlemci	2 Core
Bellek	1 GB
Kapasite	20 GB
Network	1 adet network adaptörü

Tablo 2.5. Kali Linux ve Windows 10 Pro Sanal Makine Özellikleri

BÖLÜM III
SİSTEM ENTEGRASYONU VE TEST

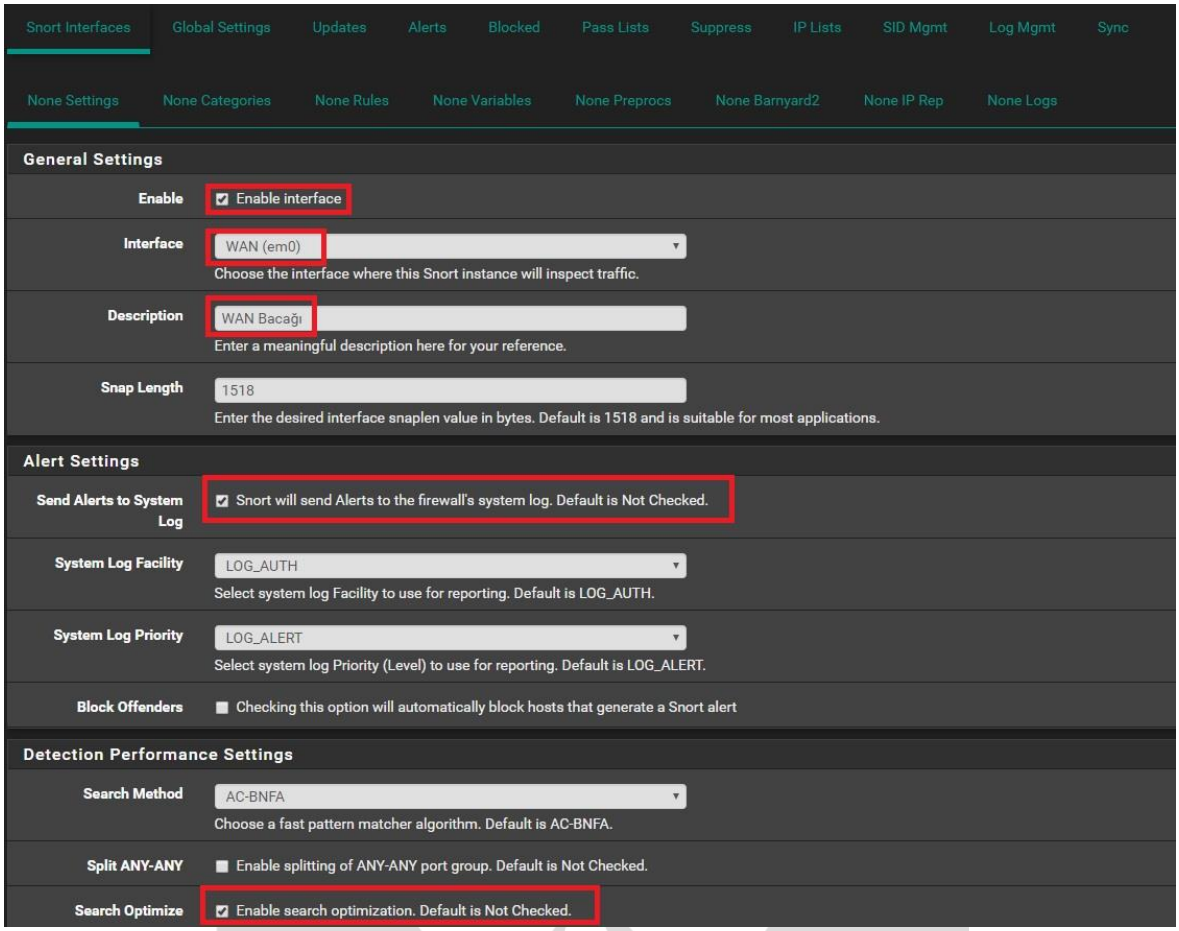
3.1. Snort Aktif Etme

Kurulumu, aktif edilen oinkcode key sayesinde güncellenmesi yapılan snort'un aktif edilmiştir. Snort wan ve lan bacakları ile ilgili olarak ayarlamalar yapılarak loglama için hazır hale getirilir. Bunun için Services (servisler) tabından snort seçimi yapılır.

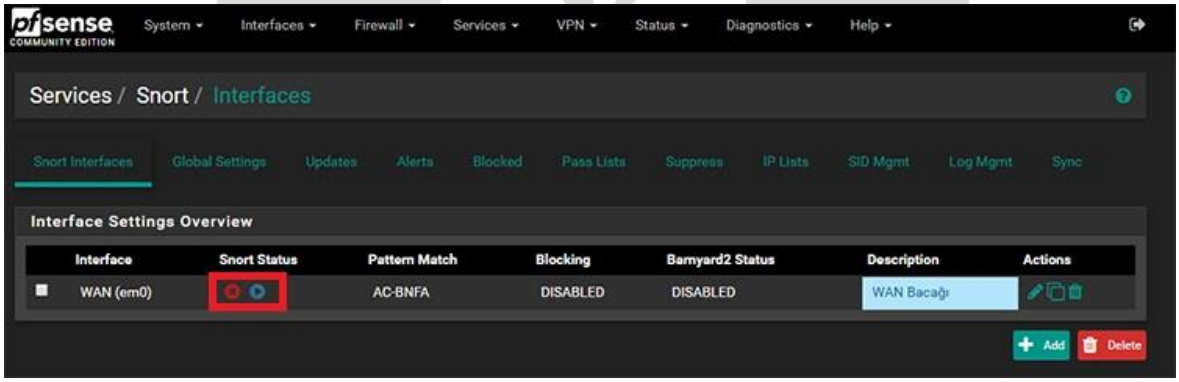


Şekil 3.1 Snort Servisi Seçimi

Gelen ekranda Snort Interfaces kısmında Add yaparak network bacaklarının ayarlamaları yapılacaktır. Öncelikli olarak Wan Network Bacağı daha sonrasında Lan Network Bacağının ayarlamaları yapılır. Şekil 3.2. ve Şekil 3.3.

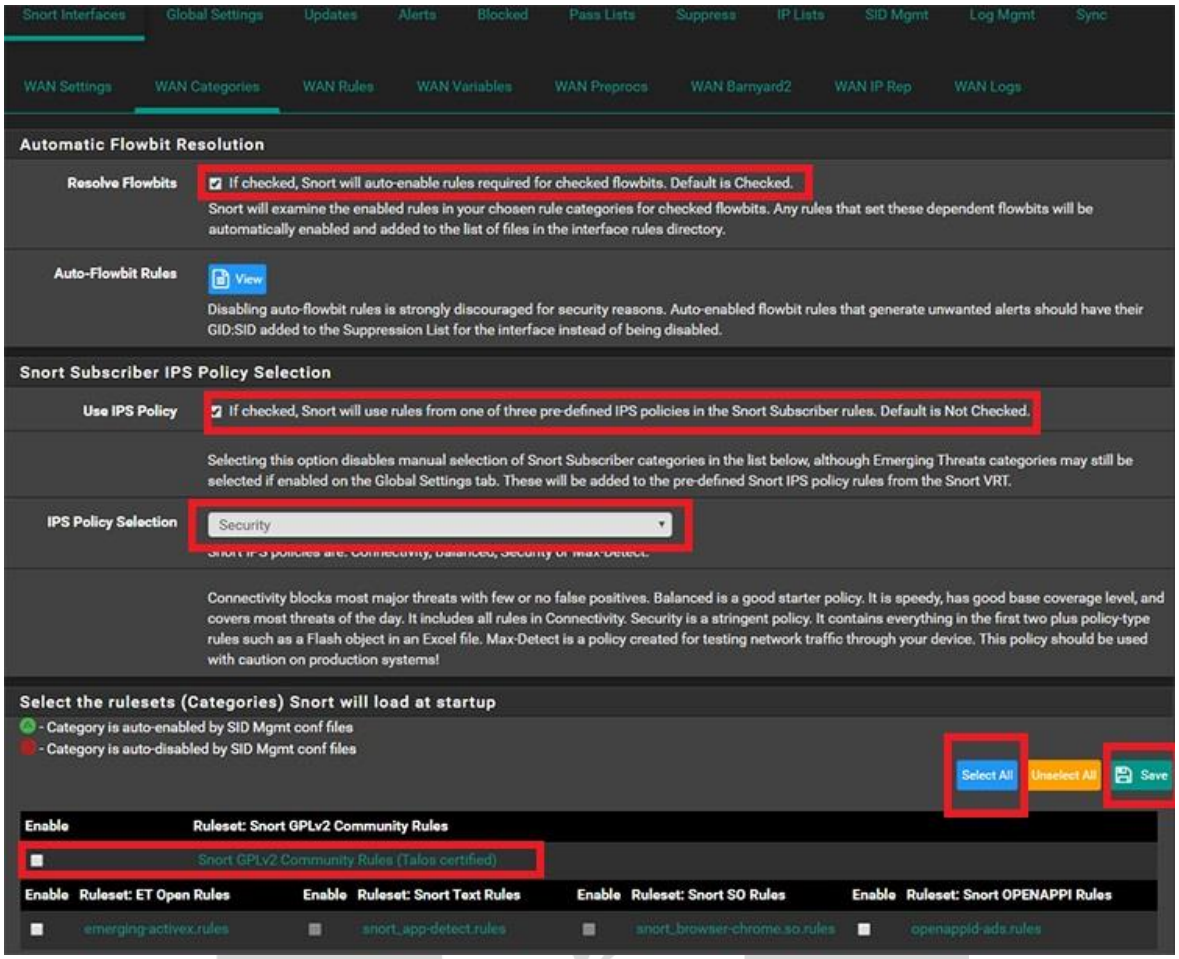


Şekil 3.2 Wan Network Bacağını Ayarlama



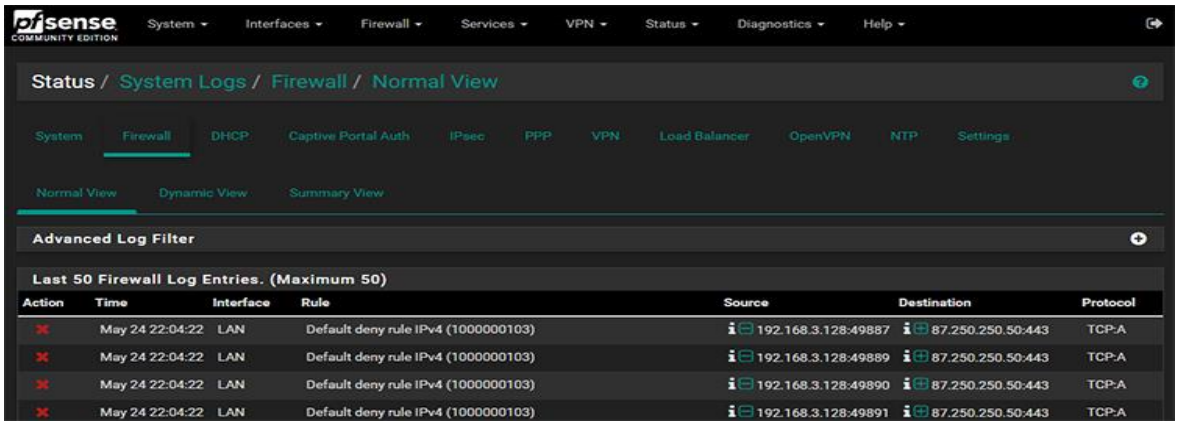
Şekil 3.3. Wan Bacağı

Network ağının hangi kurallarla korunacağı hususunda seçenekler seçimi yapılır. Community sürümünü yüklediğimizden, community kuralları aktif olacaktır. Şekil 3.4



Şekil 3.4. Wan Kategorisi Kural Seçimi

Lan bacağı ayarlamaları için aynı yöntemler kullanılmaktadır. İşlemin sonunda Şekil 3.3'te Lan bacağı eklentisi ayrıca gelecektir. Wan ve Lan bacağını Snort Status kısmından Play butonuna basarak servis başlatılacaktır. Statu -> System Logs-> Firewall ->Normal View kısmında oluşan logları görülebilmektedir. Şekil 3.5.



Şekil 3.5. Firewall Log Görüntüsü

3.2. Model Ağ Sistemine Saldırılar

Saldırılar genel anlamda öncelikli olarak oluşturulan model ağı keşif amaçlı saldırılar yapıldıktan sonra trafik saldırı ve engelleme yöntemlerine başvurulmuştur. Keşif ve saldırı sonuçları işlem esnasında değerler elde edilmiştir.

3.2.1. Keşif Saldırıları

3.2.1.1. NMAP

Nmap, ağ tarama ve zafiyet tespiti için kullanılan açık kaynaklı bir araç olup, birçok sisteme yönelik taramaları gerçekleştirerek hızlı, esnek ve anlamlı bir şekilde sonuç üretir. Sistemlerin aktif veya pasif, aktif olan sistemlerin port durumlarını, hangi servislerin çalıştığını, sistemde çalışan işletim sistemini gibi bir çok bilgiyi elde eder. [13] Nmap ile tespit edilen servislerin güvenlik açığı barındırıp barındırmadığı ve kullanılan servisler hakkında bilgi elde edilebilir. Ayrıca içerisinde barındırmış olduğu scriptler ile hedef sisteme yönelik tarama gerçekleştirildiğinde hedef sistem hakkında detaylı bilgi ve güvenlik açığı olup olmamasına yönelik sonuç üretmektedir. Nmap aracı, alanının en iyi araçları arasında yer almaktadır. Bu çalışmada nmap saldırıları gerçekleştirmeden önce keşif ve bilgilendirme amaçlı kullanılmıştır.

Snort kısmında Nmap'i tespit edecek kurallarımızı yazıyoruz. Bunun için snort web arayüzünde Wan ve Lan interface'ini seçip, Rules kısımlarına custom.rules olarak ekliyoruz.

alert icmp any any -> 192.168.3.132 any (msg: "NMAP ping sweep Scan"; dsize:0;sid:10000004; rev: 1;)

alert tcp any any -> 192.168.3.132 22 (msg:"Nmap XMAS Tree Scan"; flags:FPU; sid:1000006; rev:1;)

alert tcp any any -> 192.168.3.132 22 (msg:"Nmap FIN Scan"; flags:F; sid:1000008; rev:1;)

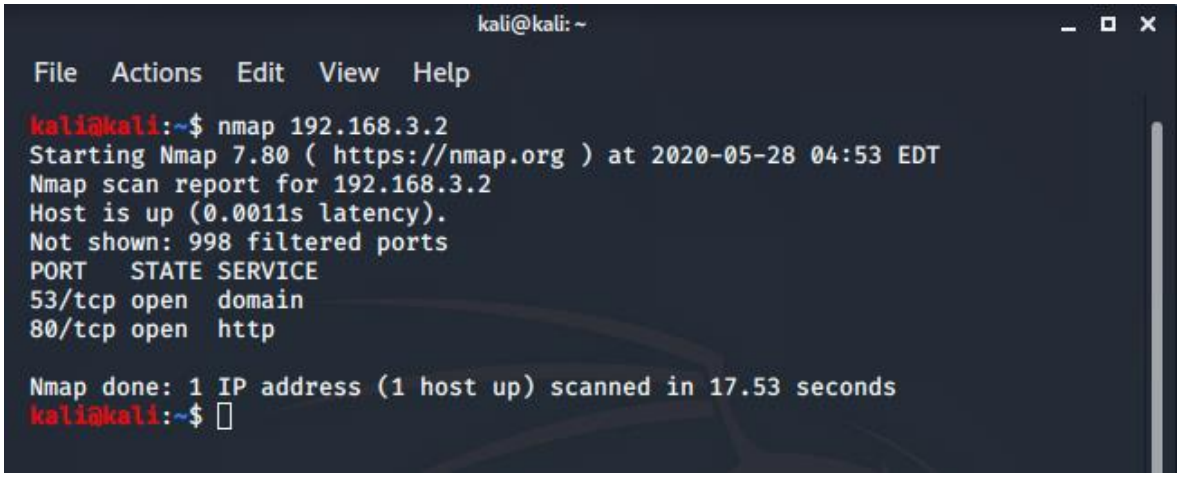
alert udp any any -> 192.168.3.132 any (msg:"Nmap UDP Scan"; sid:1000010; rev:1;)

Model ağda saldırgan olarak kullanılan Kali Linux sisteminde nmap uygulaması ile keşfe başlıyoruz;

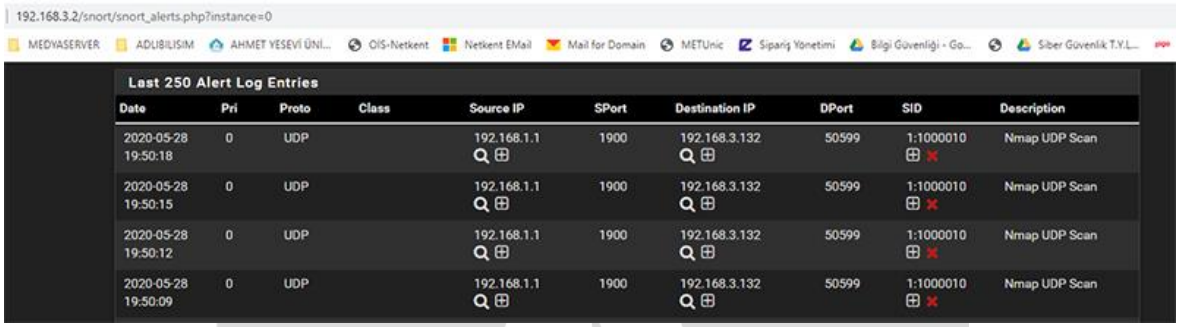
Sonuçlar aşağıda verilmiştir.

kali@kali:~$ nmap -v -sn 192.168.3.0/24
Starting Nmap 7.80 (https://nmap.org) at 2020-05-27 06:11 EDT
Initiating Ping Scan at 06:11
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 06:11, 2.54s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 06:11
Completed Parallel DNS resolution of 256 hosts. at 06:11, 13.00s elapsed
Nmap scan report for 192.168.3.0 [host down]
Nmap scan report for 192.168.3.1
Host is up (0.0019s latency).
Nmap scan report for 192.168.3.2
Host is up (0.0020s latency).
Nmap scan report for 192.168.3.3 [host down]
.
Nmap scan report for 192.168.3.132 / Windows 10 pro*
Host is up (0.010s latency).
Nmap scan report for 192.168.3.131
Host is up (0.000091s latency).
.
.

Gelen sonuçlara göre ağda aktif olan makinaları, cevap verme süreleri bulunmaktadır. Aktif olarak tespit edilen makinalara ait açık port ve diğer bilgilerini almak üzere nmap ile paket göndermeye çalışacağız. Nmap komutunun icrası sonucu aşağıda belirtilmiştir.



Şekil 3.6. PfSense Makinasına Nmap Keşfi



Şekil 3.7. Snort Nmap UDP paketlerinin tespiti

3.2.2. ATAKLAR

Distributed Denial of Service (Dağıtık Hizmet Engelleme-DDoS) saldırıları, belirli bir sunucuyu veya çevrimiçi hizmeti sınırlamak ya da tamamen ortadan kaldırmak için saldırganlar tarafından yapılan saldırılardır. DDoS saldırılar, genel çerçevede "zombi" makineler kullanılarak oluşturulan "botnetler" ile gerçekleştirilir. Saldırganların kendilerini tehlikeye atmadan, gizleyerek ve işlem gerçekleştirmelerini kolaylaştırarak saldırı ağlarını güçlendirmesini sağlayan bu sistem DDoS saldırıları için önemli bir kaynak oluşturmaktadır. [14]

Web sunucuları gibi ağ kaynaklarının da eş zamanlı olarak hizmet verebileceği isteklerin sayısı, sunucunun kapasite sınırına ek olarak sunucuyu internete bağlayan bağlantı da sınırlı bir bant genişliğine sahiptir. İstek sayısı altyapıdaki herhangi bir bileşenin kapasite sınırını her aştığında hizmet düzeyi büyük olasılıkla aşağıdaki sorunlardan biriyle karşılaşır:

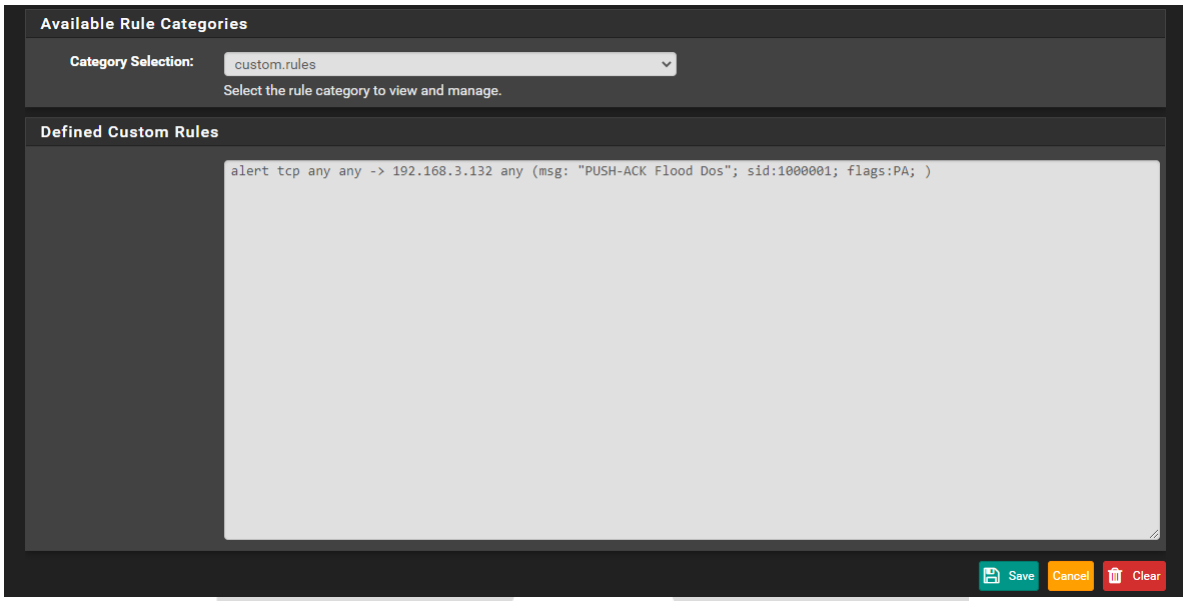
- İsteklere verilen yanıtlar normalden çok daha yavaş olur.
- Bazı (veya tüm) kullanıcı istekleri tamamen zaman aşımına uğrar.

Genellikle saldırganın başlıca amacı sunucu kaynağının normal çalışmasını tamamen engellemektir. Çoğu zaman saldırgan, saldırıyı durdurması karşılığında para da isteyebilir. Bazı durumlarda DDoS saldırısının amacı rakip bir firmanın itibarını zedeleme ya da işine zarar vermek de olabilir. Başlıca DDoS atak tipleri aşağıda belirtildiği gibi açıklamaları ve bazı örnek ataklar yapılarak, Snort sisteminde alarmları üretecek roller eklenecektir. [16]

- SYN Flood
- SYN-ACK Flood
- ACK or ACK-PUSH Flood
- Fragmented ACK Flood
- RST/FIN Flood
- XerXes Fake Session Attack
- UDP Flood
- UDP Fragmentation Flood
- Non-Spoofed UDP Flood
- ICMP Flood
- ICMP Fragmentation Flood
- Ping Flood
- IP Null/TCP Null Attack
- DNS Flood DNS Amplified
- Slow Session Attack
- Slow Read Attack
- HTTP Fragmentation
- HTTP GET Flood
- Recursive GET
- Random Recursive GET
- Specially Crafted Packet
- NTP Flood

3.2.2.1. ACK-PUSH Atak

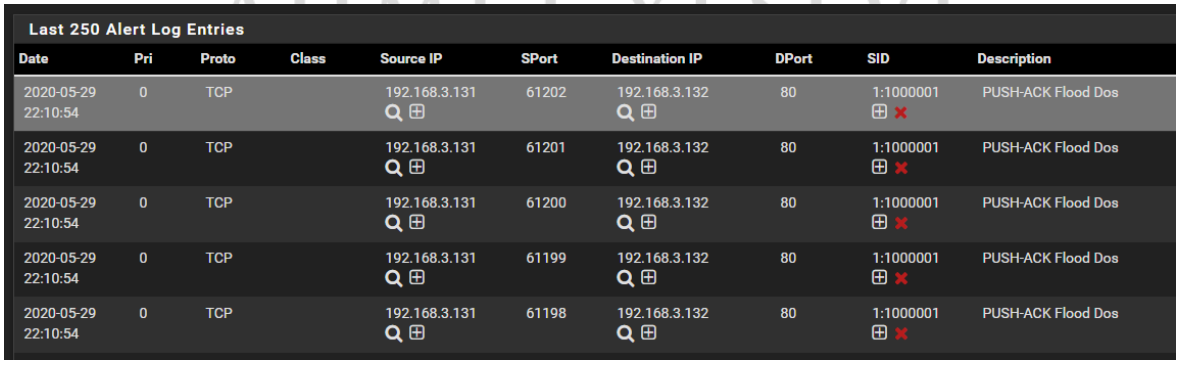
Kaynak tüketimine yönelik saldırılardan biri olan ACK-PUSH sızma amaçlı gönderilen yüksek paket oranları; sunucu üzerinde bulunan bağlantı listesi ve firewall üzerinde geçerli oturumları başarısızlığa uğratmak amacı ile çalışmaktadır. Snort uygulamasına saldırının tespiti için gerekli rol girişi yapılır.[16] Şekil 3.8.



Şekil 3.8. Custom Rol Giriş Ekranı

Push ACK Flood atağını yapmak için ekrandaki komut girilir. Bu komut Windows 10 Pro kurulumlu sanal makinada 80 nolu porta paket gönderimi yapar.

"hping3 -PA --flood -p 80 192.168.3.132"



Şekil 3.9. Snort Arayüzü Push Attack

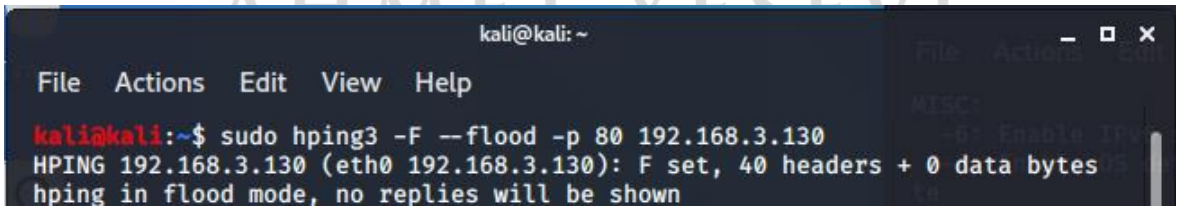
3.2.2.2. UDP Atak

Saldırgan Sanal Makinadan kaynakta bulunan IP range üzerinden yüksek kapasiteli sahte UDP paketleri göndermektedir. Hedef network(Router'lar, Firewall'lar, IPS/IDS cihazları, WAF ve sunucular) yüksek kapasitede ve yüksek sayıda gelen UDP paketlerinden çökmeye başlar ve mevcut hedef network'ü kapanmaya zorlar. [16]

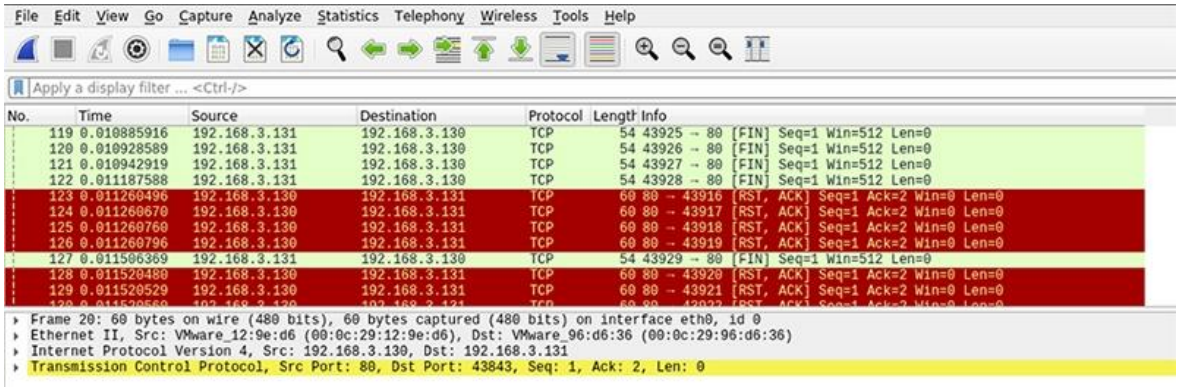
Saldırı topolojimizde yer alan Kali Linux İşletim sisteminden Windows 10 pro işletim sisteminde IIS (Internet Information Service) kurulu sisteme yapılacaktır. Güvenlik duvarımıza "*alert udp any any -> 192.168.3.132 any (msg: "UDP Flood Dos"; sid:1000001;)*" rolünü custom.rules kısmına ekliyoruz. Burada amacımız UDP paketlerini gönderip, servisi meşgul etmektir.

Şimdi de hping3 uygulamasını deneyeceğiz. Hping3 uygulaması linux sistemleri üzerinde kurulabilen bir güvenlik uygulaması olup, kali sistemimizde paket kurulu halde gelir. Bu uygulamayı kullanarak daha çok firewall, ips ve Anti-DDoS cihazları test edilir. Tabi kullanım amacına göre değişmektedir. Uygulama genel olarak IP spoofing yaparak hedef sistemi korumak için kullanılan cihazların aktif oturum limitlerini doldurup, hizmetin servis veremez hale getirmeyi hedeflemektedir. Komutumuz sonsuz sayıda sisteme sonsuz sayıda paket göndermeye çalışacaktır.

hping3 -F --flood -p 80 192.168.3.132



Şekil 3.10. Hping3 paket gönderme



Şekil 3.11. Wireshark ile gönderilen paketler listesi

Söz konusu saldırı Snort sisteminde gönderilen paketler tespit edilmiştir. Windows 10 Pro üzerinde çalışan 80 portlu IIS çalışmaya devam etmiştir.

Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2020-05-29 21:02:44	0	UDP		192.168.3.131	43055	192.168.3.132	80	1:1000001	UDP Flood Dos
2020-05-29 21:02:44	0	UDP		192.168.3.131	43054	192.168.3.132	80	1:1000001	UDP Flood Dos
2020-05-29 21:02:44	0	UDP		192.168.3.131	43053	192.168.3.132	80	1:1000001	UDP Flood Dos
2020-05-29 21:02:44	0	UDP		192.168.3.131	43052	192.168.3.132	80	1:1000001	UDP Flood Dos
2020-05-29 21:02:44	0	UDP		192.168.3.131	43051	192.168.3.132	80	1:1000001	UDP Flood Dos

Şekil 3.12. Snort Güvenlik Duvarı

Şekil 3.13. Internet Information Services web arayüzü

3.2.2.3. RST / FIN Atak

Saldırgan, Firewall'a doğru durum tablolarına/sunucunun tablolarına herhangi bir oturuma ait olmayan yüksek oranda RST / FIN paketleri gönderir. RST ve FIN Flood saldırıları hedef sunucu/Firewall'ın paketleri karşılaştırmak üzerine çalışırken kaynakları tükenir. Tükenen kaynaklar ile saldırı başarıya ulaşmış olur. [16]

Güvenlik Duvarına (Snort) bu saldırıyı karşılayacak rol tanımlanır.

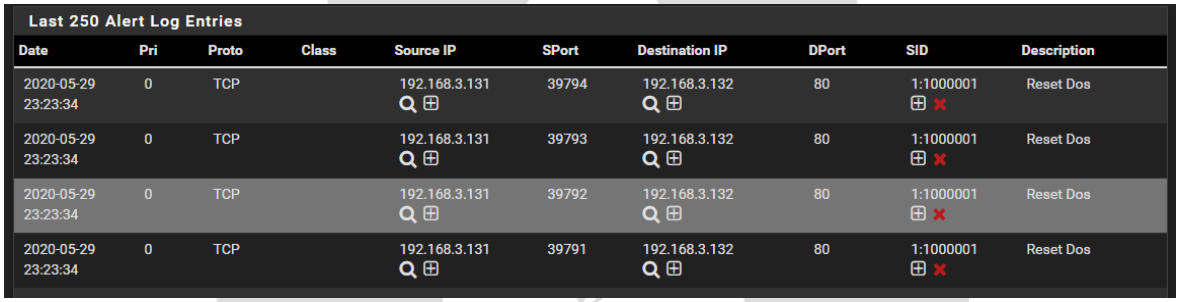
"alert tcp any any -> 192.168.3.132 any (msg: "Reset Dos"; sid:1000001; flags:R;)
"alert tcp any any -> 192.168.3.132 any (msg: "FIN Dos"; sid:1000001; flags:F;)"

Saldırgan hping3 uygulamasını kullanarak aşağıdaki komutu icra eder.

"hping3 -R --flood -p 80 192.168.3.132" / Reset Dos*

"hping3 -F –flood -p 80 192.168.3.132" / Fin Dos*

Snort alarmı aşağıda listelenmiştir.



Şekil 3.14. Reset Dos Atak

3.2.2.4. ICMP Atak

DDOS saldırganları kaynakta bulunan IP range üzerinden yüksek kapasiteli sahte ICMP paketleri göndermektedir. Hedef ağdaki kaynaklar gelen yüksek sayıda ICMP paketlerine dayanamaz ve network offline duruma geçer. [16]

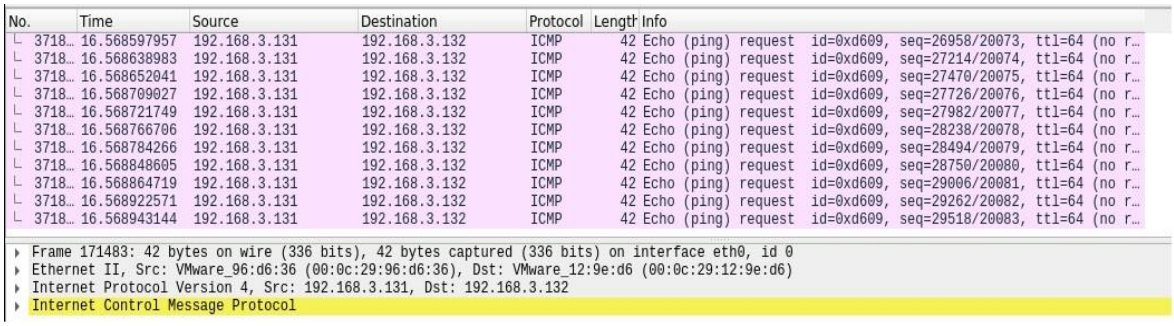
Güvenlik duvarına (Snort) saldırganın yapacağı bu atağa karşı alarm rolümüzü tanıtıyoruz.

"alert icmp any any -> any any (msg: "Smurf Dos Attack"; sid:1000003;itype:8;)"

Saldırgan aşağıdaki komutu icra etmektedir.

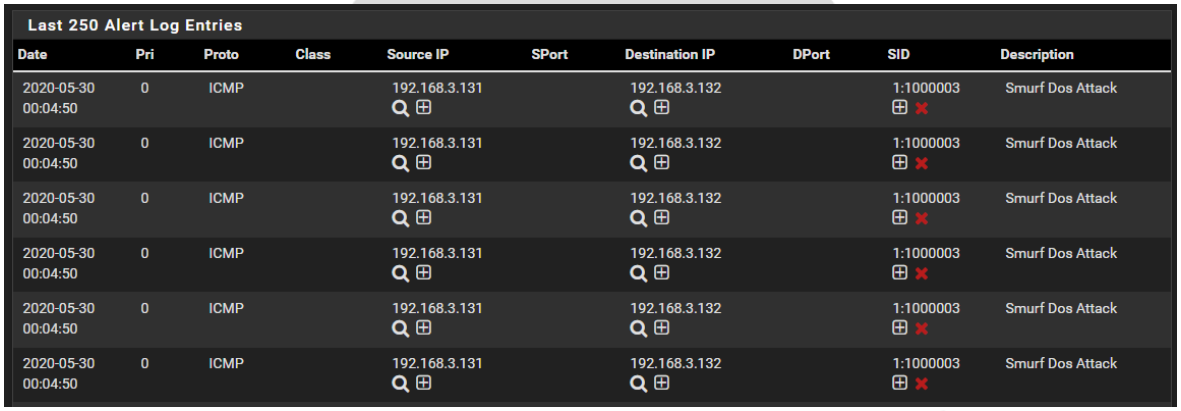
"hping3 --icmp --flood -c 1000 --spoof 192.168.3.131 192.168.3.132"

Gönderilen paketler Wireshark aracı ile gözlemlenmiştir. Şekil 3.15.



Şekil 3.15. Wireshark ICMP atakları

Snort saldırılar karşısında alarm üretmektedir. Şekil 3.16.



Şekil 3.16. Snort ICMP atakları

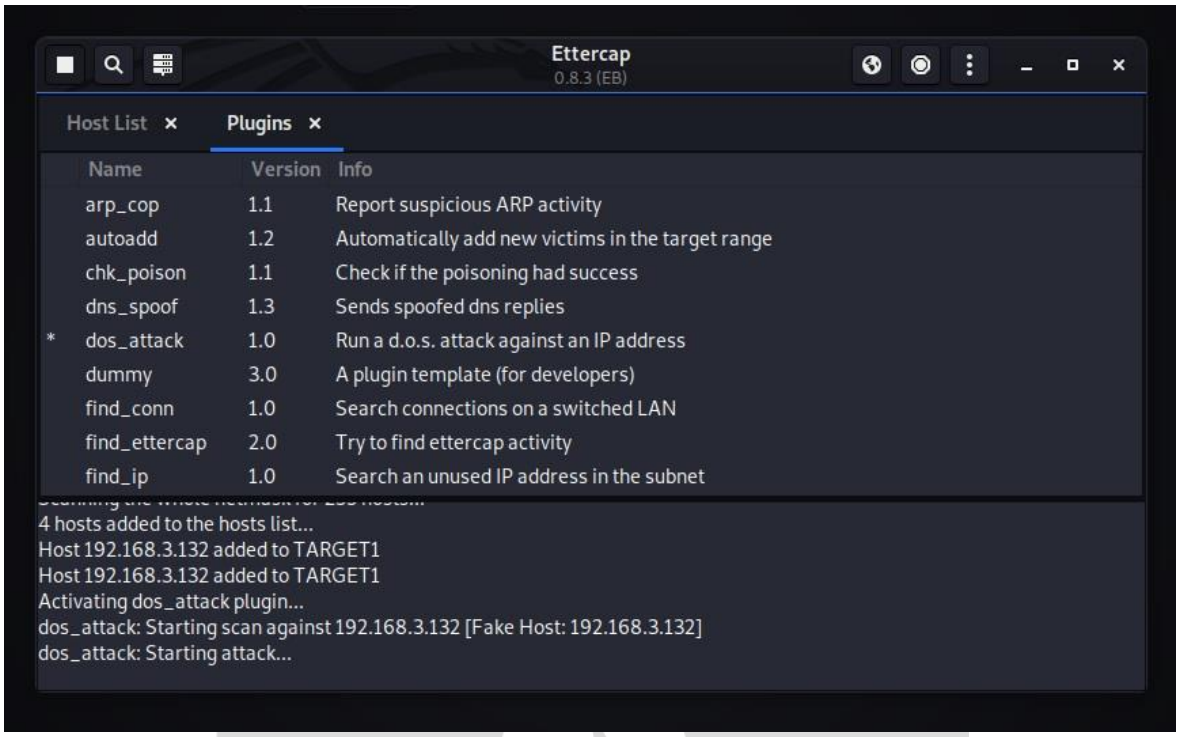
3.2.2.5. TCP SYN Atak

SYN Flood tipi DDOS ataklar genellikle Firewall(güvenlik duvarı), IPS/IDS ve tüm ağa ait olan bant genişliğini tüketmek amacı ile kullanılır. SYN Flood DDOS saldırısı ile saldırı yapılan sunucu (IP)/Firewall biriken yük ile reboot edilmeye zorlanacaktır. [16]

Güvenlik Duvarına (Snort) atak alarm rolünü eklenir.

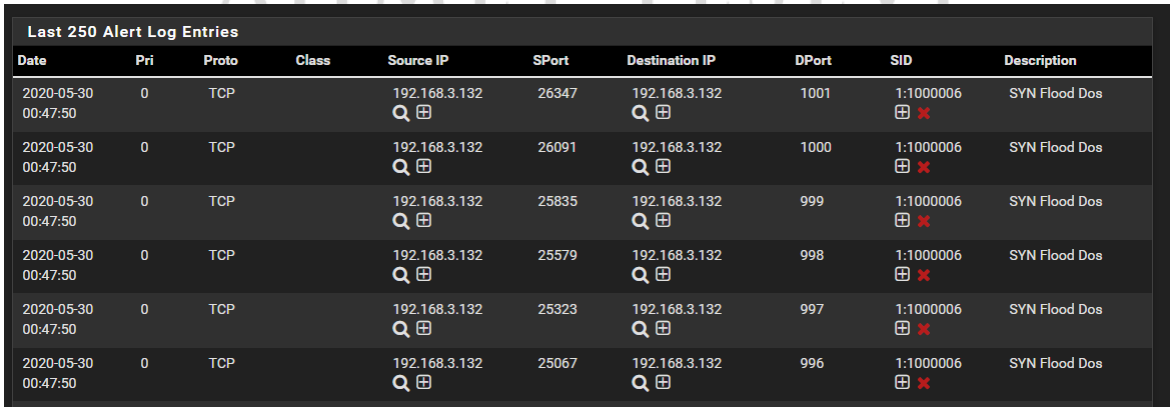
"*alert tcp any any -> 192.168.3.132 any (msg:"SYN Flood Dos"; flags:S; sid:1000006;)*"

Saldırgan atak yapmak için ettercap uygulamasını kullanmaktadır. Ayrıca atağı fake dediğimiz yalancı IP adresi ile karşı tarafın IP adresi ile yapmaktadır. Şekil 3.17.



Şekil 3.17. Ettercap dos_attack

Saldırı sonucunda daha önce tanımlanan alarm rolünü snort tanımlayarak alarmı vermektedir. Şekil 3.18.



Şekil 3.18. Snort Ettercap Dos Atağı alarmı

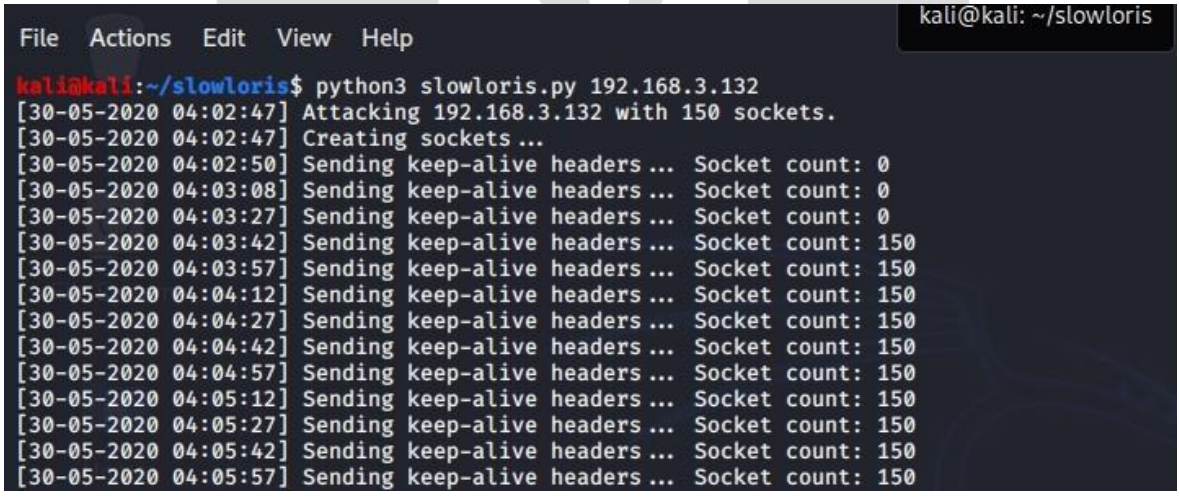
3.2.2.6. Slowloris Session Atak

Slow session attack'lar hedefte bulunan bilgisayarı uzun periyodlarda açık tutmak ve cihazı yormak amacıyla yapılan bir ataktır. Saldırganlar TCP-SYN paketleri gönderir TCP three-way handshake'e neden olur, ACK paketleri SYN paketlerinden daha uzun periyotlarla gönderim yapar. [16]

Güvenlik duvarına daha önceden tanımlanan SYN Flood alarm rolü tanımlanmıştır. Bu atağı yapmak için öncelikle Kali Linux'a Python ile hazırlanan slowloris.py uygulamasını github kod ve uygulama paylaşım platformundan indirilmektedir. Şekil 3.19.

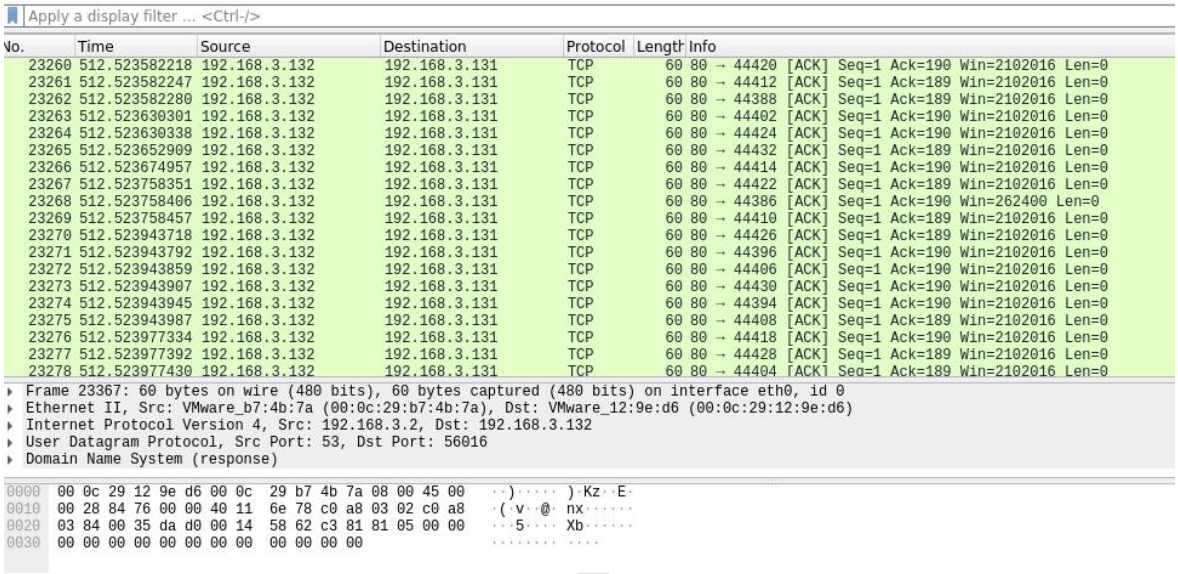
Şekil 3.19. Slowloris indirme

Slowloris uygulaması atak için kullanılır. Şekil 3.20.



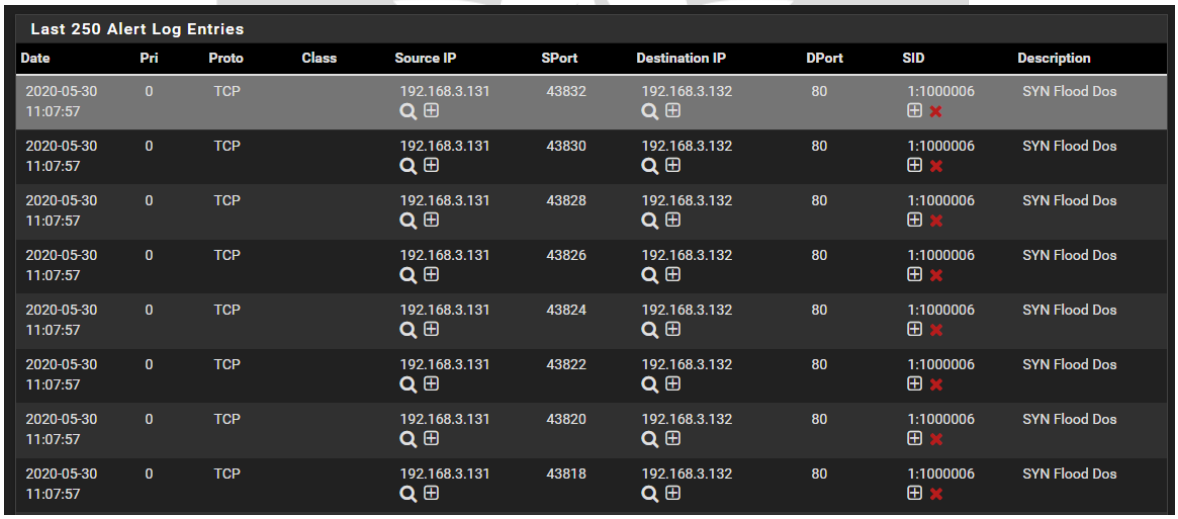
Şekil 3.20. Slowloris Atak

Wireshark ile gönderilen paketler izlenir. Şekil 3.21.



Şekil 3.21. Wireshark Slowloris paketleri

Snort güvenlik duvarın daha önceden tanımlanan SYN Flood rolü alarm vermektedir. Şekil 3.22.



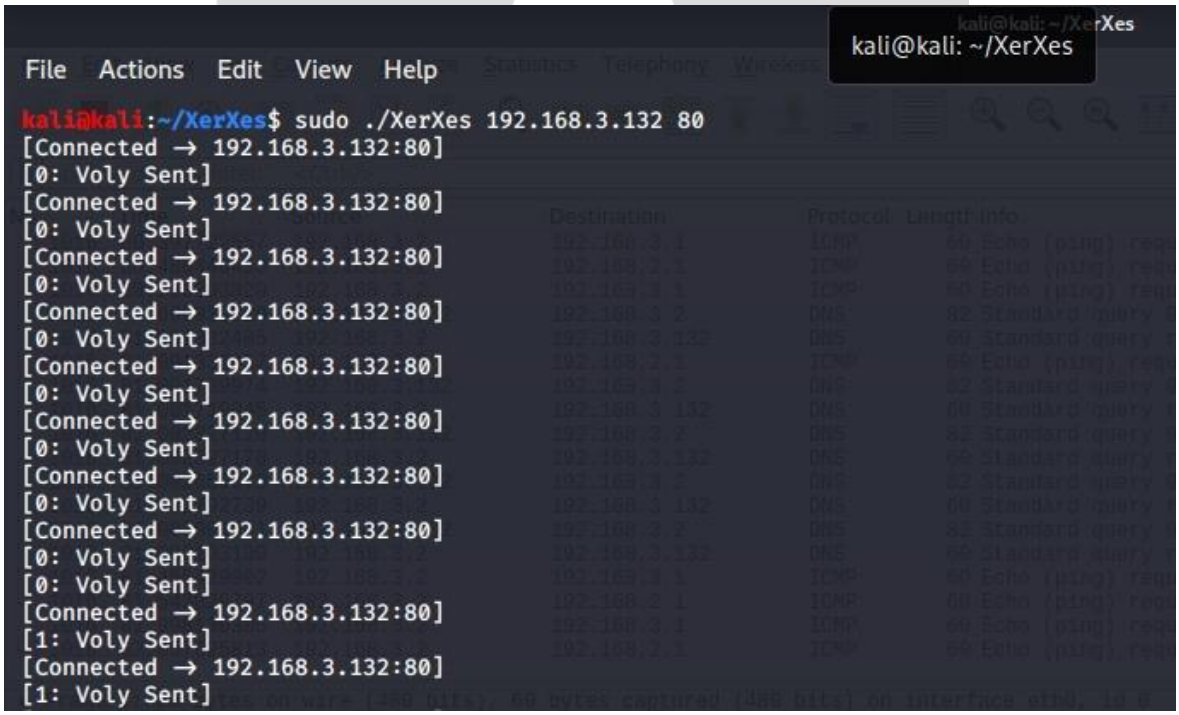
Şekil 3.22. Snort Slowloris Alarm

3.2.3.7. Xerxes Yalancı (Fake) Session Atak

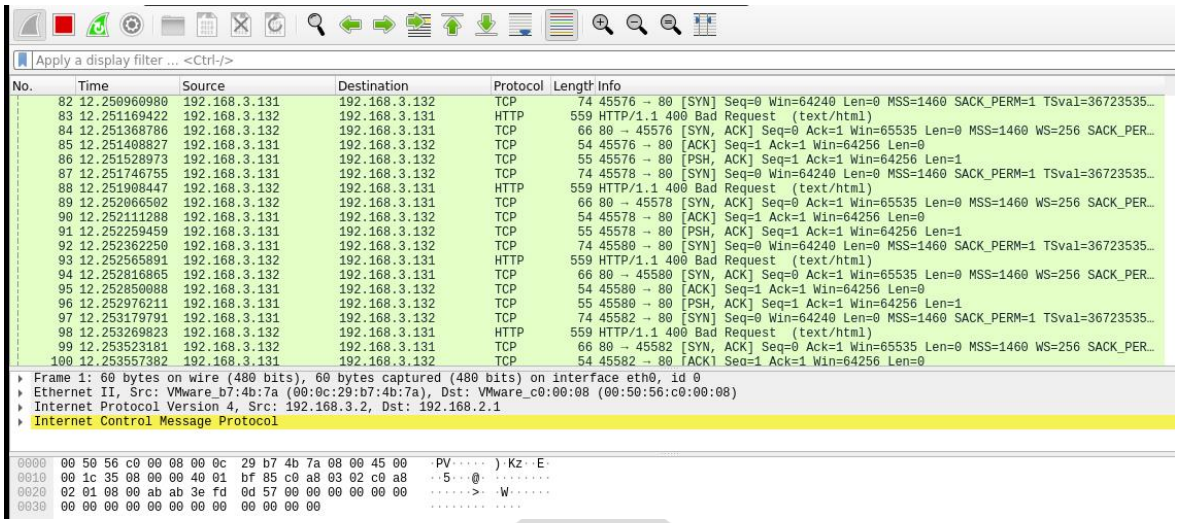
Saldırganlar sahte SYN paketleri, çoklu ACK paketleri ve sonrasında bir veya birden çok RST/FIN paketi göndererir. Bu paketler birlikte görüldüğünde tek bir TCP session olarak algılanmaktadır. Hedefte bulunan sunucu gelen cevapları ayıklamaya çalışırken bütün kaynaklarını tüketecektir. [16]

Xerxes saldırısı yapmak için github platformundan xerxes C kodunu indirip sistemde GCC compile "sudo gcc xerxes.c -o xerxes" ile hazır hale getirilerek saldırı yapılır.

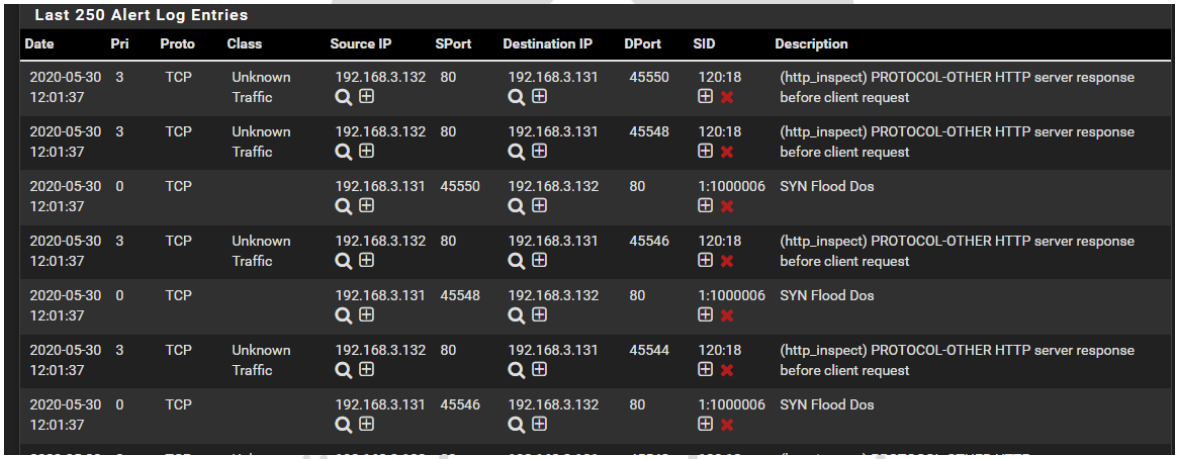
Şekil 3.23. Xerxes uygulmasını github platformundan indirme



Şekil 3.24. Xerxes Atak



Şekil 3.25. Wireshark Xerxes paket gönderme görüntüsü



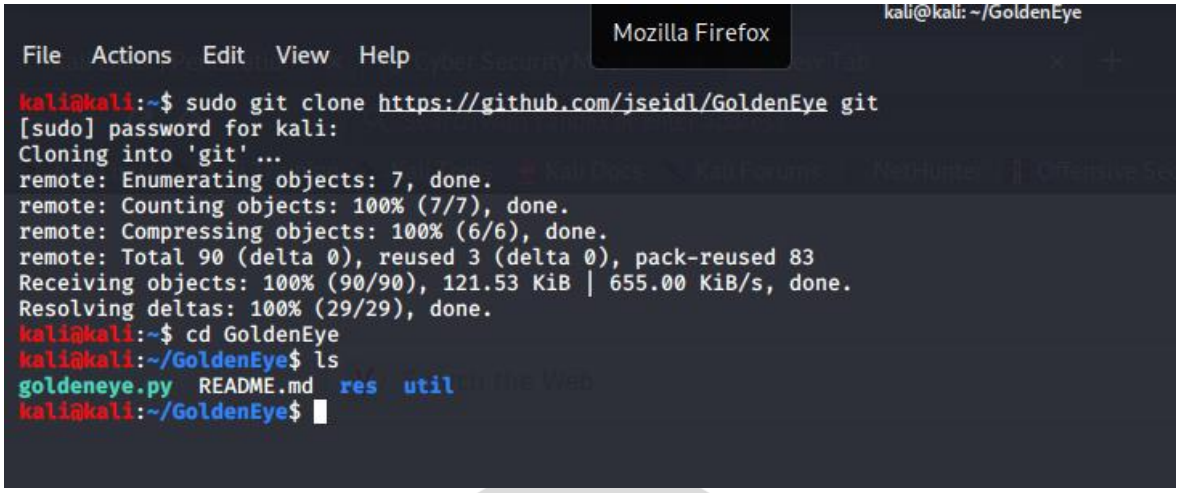
Şekil 3.26. Snort Xerxes alarmı

3.2.2.8. Golden Eye (Altın Göz) Atak

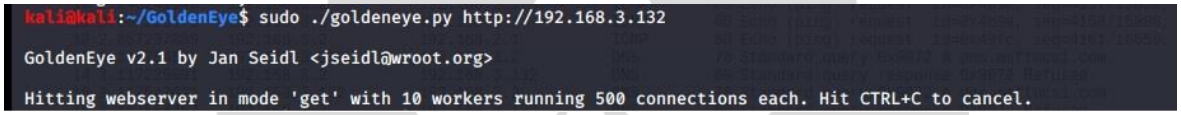
Bu saldırı uygulaması Jean Seadl tarafından python da geliştirilmiş olup, hedef bilgisayara TCP Syn paketleri oluşturup, belirtilen porta ataklar yapmaktadır. Güvenlik Duvarına (Snort) atağı karşılayacak alarmı custom.rules kısmından oluşturuyoruz.

"alert TCP any any -> 192.168.3.132 any (msg: "TCP Flood"; sid:1000001;)"

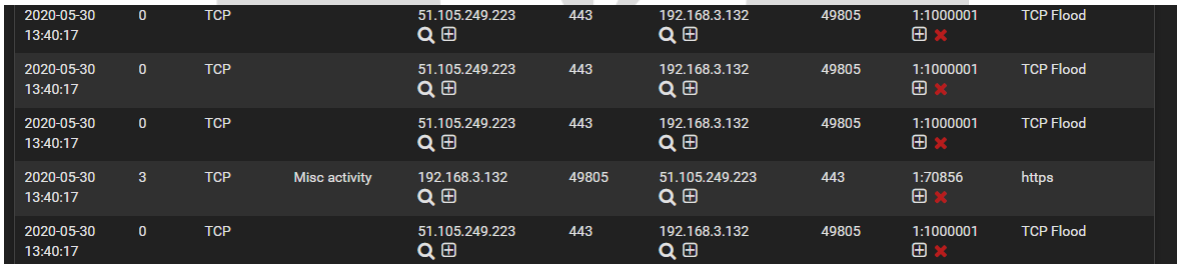
Saldırı uygulaması Kali Linux'a github platformu üzerinden indirilir ve saldırı yapılır. Snort bu konuda alarm üretecektir. Şekil 3.27, Şekil 3.28, Şekil 3.29.



Şekil 3.27. GoldenEye uygulamasını github platformundan indirme



3.28. GoldenEye Atak.



3.29. GoldenEye Snort Alarm.

3.3. Ek Olarak Yapılabilecek Ataklar

3.3.1 Zaman, Ajan adı ve Port Numarası Değiştirme [20]

Snortta oluşturulan roller ve kurallar konusunda saldırılarda belirli parametrelerin değiştirilmesi ile saldırı tespit ve engelleme sisteminin atlatılması, saldırı aşamasının keşif bölümünde uygulanabilen bir atlatma tekniğidir. Temel amaç saldırı tespit ve engelleme sisteminin baktığı ana saldırı bulgularını farklılaştırarak sistemi atlatmaktır. Ek olarak zaman, ajan adı ve port numarasına göre imzalar ve desenler (pattern) mevcuttur. Bu parametreler ile oynamak saldırı tespit ve engelleme sisteminin korelasyon ve tespit motorlarını yanıltmaktadır.

Zamanı değiştirme tekniği zamanı yavaşlatma olarak kullanılmaktadır. Bu teknikte TCP tarama esnasında 4 senaryo uygulanabilmektedir; [16]

İlk senaryo: Saldırgan makine bir SYN paketi gönderir ve hedeften bir SYN-ACK alır. Bu, bağlantı noktasının açık olduğu ve farklı bir bağlantı noktasına geçtiğimiz anlamına gelir. Her portun saldırganı kandırması için bir SYN-ACK paketi gönderen bir yazılım olması çok düşük bir ihtimaldir, ancak bu olası değildir.

İkinci senaryo: Saldırgan bir SYN paketi gönderir ve bir ICMP bağlantı noktasına ulaşılamıyor iletisini geri alır, bu büyük olasılıkla bağlantıyı engelleyen güvenlik duvarı olduğu anlamına gelir. Bu bağlantı noktalarına filtrelenmiş bağlantı noktaları da denir.

Üçüncü senaryo: Saldırgan makine SYN paketi gönderir ve bir RST-ACK paketi geri alır, yani bağlantı noktasına ulaşamayız, kapalı veya bir güvenlik duvarı buna erişmemize izin vermez.

Dördüncü senaryo: Saldırgan makine SYN paketi gönderir ve yanıt almaz, genellikle bağlantı noktası tarama araçları devam etmeden önce yeniden dener ve bağlantı noktası filtrelenmiş olarak işaretlenir. Bu durumda, ya son sistemde (tüm paketleri sessiz bir şekilde kapalı bağlantı noktalarına sessizce bırakmak üzere yapılandırılmış) hiçbir şey dinlemez ya da bir güvenlik duvarı gelen SYN paketimizi engeller (yine sessizce reddeder).

Bunlar, bağlantı noktası taraması sırasında karşılaşacağınız en olası senaryolardır; son senaryo, aracın yeniden uzun süre çalışmasına neden olabilir, çünkü yeniden dener ve zaman aşımından sonra filtrelenmiş olarak işaretler. Bu tekniğe yarı açık tarama da denir. Tam bir bağlantı kurmuyoruz.

Hepimizin bildiği gibi UDP bağlantısız bir protokoldür, bu nedenle bağlantı durumu ve kontrol biti yoktur ve bu nedenle daha az tarama seçeneği, genellikle daha yavaş tarama ve daha az güvenilir tarama ve sonuçlardan çok fazla belirsizlik vardır. UDP taramasında karşılaşabileceğiniz bazı senaryolar:

Senaryo A: Saldırgan makine bir UDP paketi gönderir ve hedef makine bir UDP paketiyle yanıt verir. bu, UDP bağlantı noktasını dinleyen bir şey olduğu anlamına gelir, bu da bağlantı noktasının açık olduğu anlamına gelir.

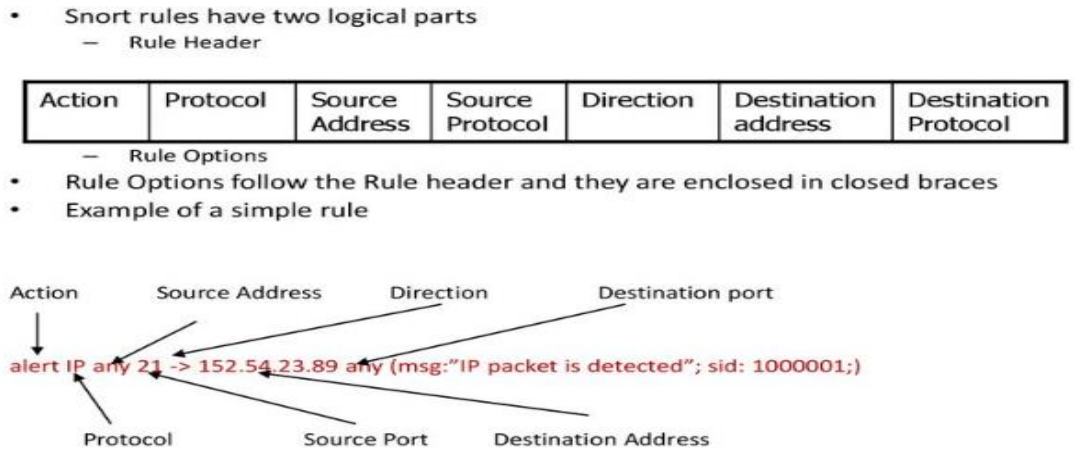
Senaryo B: Saldırgan makine bir UDP paketi gönderiyor ve hedef makineye erişilemeyen bir ICMP bağlantı noktasıyla yanıt veriyor, Bu bağlantı noktasının yakın olduğu anlamına geliyor, ancak bu aynı zamanda UDP taramasının yavaş olmasının nedenlerinden biri. - taramayı daha da yavaşlatan ICMP Paketleri için sınırlama.

Senaryo C: Saldırgan makine bir UDP paketi gönderiyor ve hiçbir şey geri gelmiyordur.

Ajan adı, HTTP/HTTPS protokollerinde bulunması zorunlu bir parametredir. Ajan adı değiştirme atlatma tekniği HTTP/HTTPS protokollerinde uygulanan bir tekniktir. Saldırganlar, saldırı araç ve programlarını varsayılan ajan adı ile kullandığında saldırı tespit ve engelleme sistemleri sadece ajan adına bakarak saldırıyı kolayca tespit edebilir. Saldırı tespit ve engelleme sistemleri güncellenen imza kümeleri sayesinde her türlü saldırı aracının ajan bilgisini bulundurmaktadırlar. Saldırgan bu ismi değiştirmediği takdirde, saldırı aracıyla yasal bir istek yapsa bile sistem bunu saldırı olarak algılayıp engelleyecektir. [17]

Farklı bir port kullanmak ya da diğer ismiyle port numarasını değiştirmek demek saldırı paketlerinde OSI ağ katmanın 4. katında değişiklikler yapmak demektir. Saldırı tespit ve engelleme sisteminde çoğu kural port bazlı yazılır ve tespit motoru da saldırıları kurallar sayesinde port bazlı olarak algılar. Bu noktada port numarası değiştirmek saldırı tespit ve

engelleme sistemini atlatmanın etkili bir yönetimidir. Bu atlatma tekniği uygulama yöntemi açısından önceden belirtilen atlatma tekniklerinden farklıdır. Bu teknikte saldırgan kendi saldırdığı portu değil kurban makinenin portlarını değiştirmelidir. Çünkü saldırgan saldırı esnasında herhangi bir portunu kullanabildiğinden sistem burada kurban makinenin portunu baz alır. Örnek olarak; saldırgan kurban makineden kendisine bir kabuk açacağı zaman HTTP gibi zaten kendisine veri akışı olan bir port kullanarak sistemi atlatabilir. Çünkü saldırı tespit ve engelleme sistemi 80 portundan dışarı yönlü yapılan veri akışını normal karşılayacağı için saldırganın bu portu kritik verileri kaçırmak için kullandığını tespit edemeyecektir.[18] Saldırı tespit ve engelleme sistemleri için port numarasının önemi ve nasıl kullanıldığı Şekil 3.30'de aşağıda gösterilmektedir.



Şekil 3.30. Örnek Snort Kuralı (https://slideplayer.com/slide/13774900/)

3.3.2.Test Ortamı ve Saldırı

Tüm testler sanallaştırma ortamı kullanılarak yapılmıştır. Sanallaştırma ortamı olarak VMware ürün ailesinden Workstation platformu kullanılmıştır. Saldırgan makine olarak bir adet Kali Linux 2020.2 versiyonu kullanılmıştır. Saldırıları iletmesi için bir adet virtual switch ve kurban makine olarak da Windows 10 Pro işletim sistemli bir makine kullanılmıştır. Saldırılar tüm port aynalama alınarak saldırı tespit ve engelleme sistemi olarak kullanılan Snort 2.9.45 sürümlü Pfsense yüklü bir makineye gönderilmiştir. Snort sisteminde alınan alarmlar Graylog üzerinden listelenmiştir. Snort sistemi FreeBSD üzerine kurulmuştur. Test ortamının mantıksal topolojisi Bölüm 2.4'te Şekil 2.2.'de verilmiştir.

Test süreci boyunca çok sayıda betik ve program kullanılmıştır. Kullanılan betik ve programlar OSSTMM açık kaynak sızma testi metodolojisine göre anlatılacaktır. [19]

OSTTMM açık kaynak sızma testi metodolojisine göre saldırının üç ana aşaması mevcuttur. Bu aşamalar sırasıyla; keşif (kurban makine veya sistemler hakkında aktif ve/veya pasif olarak bilgi toplama, açıklık ve port tarama), istismar (kurban makine veya sistemde hatalı bir protokol, kod veya işlemler üzerinden istismar) ve istismar sonrası (kurban makine veya sistemlerde yetki yükseltme, bilgi çalma, değiştirme ve kalıcılık) olarak tanımlanmaktadır.

Saldırılar ilk aşamada hiçbir atlatma yöntemi kullanılmadan icra edilmiş, trafik saldırı tespit ve engelleme sistemine gönderilmiş ve alarmlar not edilip kayıt altına alınmıştır. İkinci aşamada, atlatma teknikleri kullanılabilecek saldırılar ile birleştirilerek kurban makinelere gönderilmiş ve tüm trafik saldırı tespit ve engelleme sistemine gönderilerek alarmlar tekrar not edilip kayıt altına alınmıştır. Her iki aşamada da tüm saldırılar tam pcap olarak kaydedilmiştir. Saldırılar ve atlatma tekniklerinde, saldırının veya atlatma tekniğinin kurban makinelerde istenilen etkiyi yaratıp yaratmadığı gözlemlenmiş, başarısız saldırı ve atlatma teknikleri test sonuçlarına yansıtılmamıştır.[20]

Keşif aşamasında kurban makineler hakkında bilgi toplama işlemleri gerçekleştirilmiştir. Keşif saldırıları sırasıyla ip tarama, port tarama, servis bulandırma ve açık servis tespiti şeklindedir. Keşif saldırıları uygulanırken Nmap, Burp Suite, Dirb, DNSLookUp, Nikto, Enum4Linux ve SMTPEnum betik ve programları kullanılmıştır. Bu betik ve programlar ajan adı ve port numarası değiştirme atlatma tekniklerinde kullanılmıştır. [20]

İstismar aşamasında yapılan saldırılar kod yükleme, kod çalıştırma, derin dizin gezinme, dosya içerme, kaba kuvvet, XSS saldırıları şeklindedir.

Bu saldırılarda kullanılan betik ve programlar JohnTheRipper, WFUZZ, Hydra, NetCat, BeefXSS, Burp Suite, Metasploit, Veil, Msfvenom, Havij ve Hping3 şeklindedir. Bu betik ve programlar Ajan adı ve port numarası değiştirme teknikleri ile kullanılmıştır. [20]

İstismar sonrası aşamasında yapılan saldırılar yetki yükseltme, aşamalı saldırı(pivoting), veri çalma ve kalıcılık saldırılarıdır. Bu metodda NetCat, Metasploit,Veil, Msfvenom, Powershell Empire, Mimikatz, Sshutle ve Lasagne betik ve programları kullanılmıştır. Bu betik ve programlar dosya ve dizin değiştirme, dosya başlığı değiştirme ve zaman, ajan adı ve port numarası değiştirme atlatma teknikleri ile kullanılmıştır. [20]

Yukarıda bahsedilen betik ve programlara ek olarak el ile yapılan testler, bu araştırma için özel olarak geliştirmiş olduğumuz betikler, Fragroute, TCPreWrite ve TCPReplay programları aracılığıyla yapılmıştır. Yapılan saldırılar Tablo 3.1' de aşağıda verilmiştir.

Test Aşamasında Kullanılan Saldırılar	Saldırı Kısaltması
Agresif Port ve Zafiyet Tarama	APZT
Agresif Port, Zafiyet Tarama ve Linux Betiklerini Çalıştırma	APZT-L
Agresif Port, Zafiyet Tarama ve Windows Betiklerini Çalıştırma	APZT-W
Ping Atmaksızın Port Tarama	PAPT
EternalBlue İstismar Kodu	EBK
Nmap Top 10.000 Port Tarama	NMP1
Hydra ile SSH Kaba Kuvvet	HSSKK
SMTP Servisi Dökümü	SSD
"/etc/shadow" ve "/etc/passwd" Dizinlerinin Çağırılması	DCP

Tablo 3.1. Saldırılar [20]

3.4. Saldırı Sonuçları

Saldırı tespit ve engelleme sistemini atlatma tekniği zaman değiştirme ile keşif saldırı paketlerinin kurban makinelere belirli aralıklarla yavaşlatılarak gönderimi sağlanmıştır. Saldırılar saldırı tespit ve engelleme sisteminin ara belleğinde belirli bir süre tutulacağından dolayı ne kadar yavaş gönderilirse o kadar az alarm tetikleneceği varsayılmaktadır.

Atlatma tekniği kullanılırken Nmap aracının zamanlaması kullanılmıştır. Saldırıda ilk olarak Nmap default ayarda (-T5) paket gönderim hızı ile çalıştırılmış ve saldırı NT10 olarak kaydedilmiştir ve tabloda gösterilmiştir. Bu saldırı en yaygın kullanılan ilk 10.000 portun SYN taraması ile keşfedilmesi şeklinde bir saldırıdır. Nmap aracının zamanlama fonksiyonu -T parametresi ile değiştirilebilmektedir. En hızlı tarama -T5 iken en yavaş tarama -T0 olarak gerçekleştirilmektedir. [21]

Tablo 3.2'de ilk satırdan son satıra doğru gidildikçe zamanın yavaşlatılarak yapıldığı denemelerin sonuçları görülmektedir. Tablo 3.2.'nin son satırında ise en yavaş gönderim hızı olan -T0 gönderimine ek olarak paketler daha da yavaşlatılabilmek amacıyla saldırgan makinenin ara belleğinde bekletilerek gönderilmiştir. Bu sonuçlara göre zaman değiştirme ile atlatma tekniğinin kullanım yoğunluğuyla test sonuçları arasında doğrudan bir oran kurulamasa bile, en yavaş şekilde tarama yapmanın saldırgan açısından en az alarm tetikleyen ve zamanlama kategorisinde başarısı en yüksek olan deneme olduğu gözlemlenmiştir. [21]

Saldırı Adı	Kullanılan Atlatma Tekniği	Saldırı Alarm Sayısı	Atlatmalı Alarm Sayısı	Başarı Oranı
NMP1	T4 Zamanına Yavaşlatma	92	15	85
NMP1	T3 Zamanına Yavaşlatma	92	35	72
NMP1	T2 Zamanına Yavaşlatma	92	35	72
NMP1	T1 Zamanına Yavaşlatma	92	35	72
NMP1	T0 Zamanına Yavaşlatma	92	33	70
NMP1	T0 Zamanına Yavaşlatma ve Ara Bellekte Bekletme	92	9	94

Tablo 3.2. Saldırı Denemeleri [20]

En kısa taramanın tamamlanması 1.2 saniye sürerken, en uzun tarama 14 saat 38 dakika 46 saniye sürmüştür. Zaman değiştirme atlatma tekniğinde gözlemlenen en yüksek başarı %94 iken, en düşük başarı oranı %70 olarak gözlemlenmiştir.

Ajan adı değiştirme atlatma tekniği basit ama saldırganların görünmezliğini arttıran bir tekniktir. Ajan adı değiştirme atlatma tekniğinin denemelerinde yüksek başarılar gözlemlense de negatif başarılar da görülmüştür.

Ajan adı değiştirme testinde kullanılan araçlar Hydra, DirBuster, SQLMap, SMTPEnum ve Nikto'dur. Ek olarak, el ile WEB üzerinden kod çalıştırma (command execution) saldırısı test edilmiş, ardından, Burb Suite (Vekil Sunucu) ile araya girilerek gönderilen isteğin ajan adı parametresi değiştirilmiştir. Tüm saldırıların ajan adı olarak en güncel Chrome Web tarayıcısının ajan adı kullanılmıştır. [20]

Tablo 3.3'de yukarıda bahsedilen araç ve saldırılar kısaltmalarıyla gösterilmektedir. Her bir saldırının ajan adı kısmına Chrome tarayıcısının güncel ajan adı verilerek atlatma tekniği uygulanmış ve başarı oranları yan sütunda gösterilmiştir. Test sonuçlarına göre ajan adı değiştirme tekniği başarı oranı, kullanılan saldırı ve araca göre farklılık göstermektedir. Bazı denemelerde ise atlatma başarısı saldırı başarısından daha düşüktür. Bu teknik yalnızca Hydra, Dirbuster, SQLMap ve Nikto araçlarıyla kullanıldığı zaman başarıya ulaşmıştır. Ajan adı değiştirme atlatma tekniğinin kullanımı saldırganlara her zaman avantaj sağlamadığı testlerde gözlemlenmiştir. Tablo 3.3. aşağıda verilmiştir.

Saldırı İsmi	Kullanılan Atlatma Tekniği	Saldırı Alarm Sayısı	Atlatmalı Alarm Sayısı	Başarı Oranı
HFBF	Chrome Ajan Adı Kullanılması	2810	6	100%
MCE	Chrome Ajan Adı Kullanılması	0	192	-
DIRB	Chrome Ajan Adı Kullanılması	9185	1496	83%
SMS	Chrome Ajan Adı Kullanılması	468	3306	-611%
BSMS	Chrome Ajan Adı Kullanılması	3772	2486	33%
HSBF	Chrome Ajan Adı Kullanılması	2	2	0%
SMTE	Chrome Ajan Adı Kullanılması	0	5	-
NVDS	Chrome Ajan Adı Kullanılması	25096	935	96%

Tablo 3.3: Ajan adı değiştirme atlatma tekniği deneme sonuçları. [20]

Ajan adı değiştirme atlatma tekniğinde en yüksek başarı istatistiksel hesaplama nedeni ile ilk denemedir ve oranı %99,7'un üzerinde olduğu için %100'e yuvarlanmıştır. En düşük başarı ise negatiftir ve tüm testler arasındaki en büyük negatif değişim bu test sırasında kaydedilmiştir.

Port numarası değiştirme atlatma tekniği, saldırgan açısından zor ama etkili bir tekniktir. Bu teknikte önemli olan nokta, saldırganın içeriden dışarıya çıkartacağı bilgi ve dosyalarda farklı portlar kullanma zorunluluğu olması veya saldırıyı farklı bir porta göndermesi gerekmesidir. [23]

Tablo 3.4'in ilk üç satırında kısaltması CPC olan "/etc/shadow" ve "/etc/passwd" dizinlerinin farklı üç adet porttan çağırılması sonucu elde edilen başarı oranları gösterilmektedir. Sonuçlara göre aynı saldırının farklı portlardan gerçekleştirilmesinin saldırı tespit ve engelleme sistemlerinin atlatılmasında farklı başarılar gösterdiği gözlemlenmiştir. Tablonun üçüncü, dördüncü ve beşinci satırlarında farklı saldırıların aynı porttan çağırılması dendiğinde elde edilen sonuçlar gösterilmiştir. Bu sonuçlara göre, çağırılan portun yanı sıra kullanılan saldırının da alarm tetiklemede başarı oranına etkisi olduğu görülmektedir. Saldırganın, saldırı tespit ve engelleme sistemini atlatabilmek için

hem kullanacağı saldırıya hem de hangi portu seçeceğine dikkat etmesi gerekmektedir.

Saldırı İsmi	Kullanılan Atlatma Tekniği	Saldırı Alarm Sayısı	Atlatmalı Alarm Sayısı	Başarı Oranı
CPC	Port 4444 Kullanıldı	91	10	89%
CPC	Port 3367 Kullanıldı	91	10	89%
CPC	Port 8080 Kullanıldı	91	17	81%
AHPE	Port 8080 Kullanıldı	5	0	100%
XSP	Port 8080 Kullanıldı	23	4	81%

Tablo 3.4. Port numarası değiştirme atlatma tekniği test sonuçları. [20]

Port numarası değiştirme atlatma tekniğinde gözlemlenen en yüksek başarı %100 iken, en düşük başarı oranı %81 olarak gözlemlenmiştir. Son üç testte 8080 portu kullanılarak farklılıklar gözlemlenmek istenmiştir.

BÖLÜM IV
BULGULAR VE YORUM

4.1. Birinci Araştırma sorusuna ilişkin bulgular

Açık kaynak kodlu yazılımlar konusunda platfomlarda paylaşılan doküman ve belgeler genel anlamda standart bir çerçeve de hazırlanmayıp, anlık olarak oluşan problemlerde cevap verilmiş kaynaklar olduğu detayların net bir şekilde anlaşılıp paylaşılmadığı gözlemlenmiştir.

4.2. DDoS ve DoS Ataklarına Karşı Alınabilecek Önlemler

Gönderilen sahte paketleri ayıklamak ve kaynak sunucu/IP'yi engellemek için DOS saldırılarına karşı güvenlik önlemi sağlayan ve packet filtering (paket filtreleme) yapabilen bir Firewall (güvenlik duvarı) engellemek mümkündür. Ancak firewall üzerinde yapılacak konfigürasyon mevcut yapıya uygun olarak threshold değerleri ayarlanmalıdır. Çalışmamızda yapılan ataklara karşı ayrıca Snort ve Pfsense kısmında bloklama işlemleri için gerekli roller tanımlanabilir.

4.3. Yeni Ataklara Karşılık Bulgular

Yapılan ataklar konusunda saldırı paketler kısa aralıklarla atıldığından sistemsel olarak herhangi bir anomali ile karşılaşılmamıştır. Arabellekte tutulan elemanların varsayılan arabellek büyüklüğünü ve varsayılan tutulma zamanını arttırmak gereklidir. Her ne kadar arabellek büyüklüğü ve tutulma zamanı arttırılsa da paketler saldırgan tarafından daha da yavaşlatılıp alınan önlemler yine de atlatılabilir. Ancak bahsedilen iki adet önlemin alınması saldırganların zamanlama atlatma tekniğini uygulamasını daha zor bir hale getirecektir.

4.4. Atlatma Tekniklerine Karşı Alınabilecek Önlemler

Ajan adı değiştirme atlatma tekniğine karşı IDS'te bir önlem almak mümkün değildir. Çünkü ajan adı ile saldırıyı tespit etmek saldırı tespit ve engelleme sisteminin saldırıları hızlı bir şekilde keşfedebilmesini sağlayan bir yöntemdir. Bu yöntemin haricinde hazırdaki imza kümesini de kontrol ettiği için bu tekniği önleyici bir savunma

bulunmamaktadır.

Port numarası değiştirme atlatma tekniğine karşı saldırı tespit ve engelleme sistemlerinde yapılabilecek önlem, kuralların hepsinde port numarası bölümünü tüm portlar şeklinde yapmaktır. Fakat bu yöntem saldırı tespit ve engelleme sistemi için büyük bir engel yaratacaktır çünkü imzaları işletme süresi uzayacak ve bu sebeple kapasitesinin çok altında hizmet verebilir hale gelecektir. Bu tekniğe karşı önlem almak sistemi daha zayıf bir hale getirecektir. [20]

BÖLÜM V
SONUÇ, TARTIŞMA VE ÖNERİLER

5.1. Sonuç

Günümüzde IDS sistemleri kurum ve kuruluşların siber saldırılara karşı en önemli korunma kalkanıdır. Siber kalkanın geçilmesi veya kalkanın pasif hale gelmesi durumunda saldırılara karşı sistemler savunmasız kalmaktadır.

Açık kaynak kodlu yazılımlar ile araştırmanın başında saldırı tespit ve engelleme sistemi kurulumu gerçekleştirmiş, daha sonrasında bu sistem test edilmiştir. Test sonucunda, keşif ve saldırılardan elde edilen veriler saldırı esnasında verilmiştir.

Açık kaynak kodlu yazılımlarda kurulumlar olmamakla birlikte gerekli teknik destek ve teknik insan kaynağının önemi ortaya çıkmaktadır. Bunun yanında açık kaynak yazılımların hem maliyet açısından cazip olması hem de topluluklar tarafından herhangi bir eksikliği tespit edildiğinde gerekli olan güncelleme veya çözümün daha hızlı bir şekilde ortaya çıkması açık kaynak yazılımları cazip hale getirmektedir.

5.2. Öneriler

Açık kaynak yazılımlar ile derin savunma yapılması için teknik destek anlamında insan kaynakları ihtiyacını karşılayabilecek insan kaynağı yetiştirmek gerekmektedir.

KAYNAKÇA

[1]	Doç. Dr. Mustafa Fedai ÇAVUŞ, Araş. Gör. Halenur SOYSAL KURT "Kamu Kurumlarında Açık Kaynak Kodlu Yazılımların Kullanımı" Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi Özet Yazısı
[2]	VMware, "2019 Gartner Magic Quadrant'da Lider Oldu" https://www.vmware.com/content/microsites/learn/en/304750_REG.html Erişim Tarihi: 10.05.2020
[3]	FreeBSD, FreeBSD Hakkında, https://www.freebsd.org/about.html Erişim Tarihi: 11.05.2020
[4]	Kali Linux, What is Kali Linux, https://www.kali.org/docs/introduction/what-is-kali-linux/ Erişim Tarihi: 11.05.2020
[5]	Microsoft Windows, Vikipedia Sözlük Microsoft Windows, https://tr.wikipedia.org/wiki/Microsoft_Windows, Erişim Tarihi: 11.05.2020
[6]	En Son Haber, Dünyada en çok kullanılan masaüstü işletim sistemi belli oldu, https://www.ensonhaber.com/teknoloji/dunyada-en-cok-kullanilan-masaustu-isletim-sistemi-belli Erişim Tarihi: 11.05.2020
[7]	Microsoft Windows, Microsoft Release Information, https://docs.microsoft.com/tr-tr/windows/release-information/ , Erişim Tarihi: 11.05.2020
[8]	Pfsense, Getting-Started, https://www.Pfsense.org/getting-started/ Erişim Tarihi: 11.05.2020
[9]	Snort, Snort Community, https://www.snort.org/resources#documents Erişim Tarihi: 11.05.2020
[10]	Çavuş, M.F. ve Kurt, H.S.(2017).Kamu Kurumlarında Açık Kaynak Kodlu Yazılımların Kullanımı. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, 5(3).
[11]	Şen, Şenol ve Yerlikaya Tarık, Akademik Bilişim 2013 – XV. Akademik Bilişim Konferansı Bildirileri 23-25 Ocak 2013 – Akdeniz Üniversitesi, Antalya, https://ab.org.tr/ab13/kitap/sen_yerlikaya_AB13.pdf , Erişim Tarihi: 12.05.2020
[12]	Saldırı Tespit Sistemleri, İTÜ Bilgi İşlem Dairesi Başkanlığı, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/sald%C4%B1r%C4%B1-tespit-sistemleri, Erişim Tarihi:27.05.2020
[13]	Nmap, Nmap Intoduction, https://nmap.org/, Erişim Tarihi: 28.05.2020
[14]	Kaspersky, DDoS Atağı Nedir, https://www.kaspersky.com.tr/resource-center/threats/ddos-attacks
[15]	ISSA Turkey, DoS, DDoS Atakları, https://issatr.org/dosddos-ataklari/ , Erişim Tarihi: 28.05.2020

[16]	Penetration Testing, Penetration Testing Scanning 101.3, https://www.secjuice.com/port-scanning-penetration-testing-part-three/ , Erişim Tarihi: 21.05.2020
[17]	Penetration Testing, Add Custum Header To Nicto Scan, https://www.cardinaleconcepts.com/add-custom-header-to-nikto-scan/ , Erişim Tarihi:22.05.2020
[18]	https://www.cvedetails.com/cve/CVE-2017-0143/ , Erişim Tarihi:22.05.2020
[19]	OSSTMM, Open Source Security Testing Metodology Manual, https://www.isecom.org/OSSTMM.3.pdf , Erişim Tarihi: 20.05.2020
[20]	Kılıç Hakan, Saldırı Tespit ve Engelleme Sistemlerini Atlatma Saldırıları, Bitirme Tezi
[21]	https://svn.nmap.org/nmap/docs/nmap.usage.txt/ , Alındığı Tarih: 21.05.2020