NETKENT
AKDENİZ ARAŞTIRMA VE BİLİM ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ

YAZILIM MÜHENDİSLİĞİ BÖLÜMÜ

SİBER GÜVENLİKTE AKTİF VE PASİF BİLGİ TOPLAMA ARAÇLARININ UYGULANMASI AĞA SALDIRI VE SALDIRI TESPİTLERİ YÖNTEMLERİNİN İNCELENMESİ

DÖNEM PROJESİ

HAZIRLAYANLAR
Tuncay ÖZER
Ali İsa ÖZTÜRK
Semra ALADAĞ

Danışman Hocası
Dr. Burak OLGUN

ŞUBAT – 2023

ÖZET

Bilgi teknolojilerinin kullanımının yaygınlaşması ile son zamanlarda dünyada olduğu gibi ülkemizde de siber güvenliğin önemi artmaktadır. Kullanılan donanım ve destekleyici yazılımlar kullanıcıya çeşitli faydalar sağlamakla birlikte yapısı gereği algoritmik eksiklikler ve güvenlik açıklarına da sebep olmaktadır. Bilgilerin 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. Bu durum çeşitli kurum ve kuruluşları, bireysel kullanıcıları, kurumsal web sitelerini ve sistemlerini kötü niyetli şahısların (hacker) saldırılarına açık hale getirmektedir.

Siber güvenlikte kullanılan araç ve gereçlerde güvenlik duvarları, saldırı tespit, sanal ağ, ağ trafik analizleri, olay kaydediciler, zafiyet tarayıcıları, kaynak kod güvenlik analizleri, parola kontrol gibi donanım ve yazılımlardır. Yazılımlar, ücretli olarak dağıtımı yapılabildiği gibi ücretsiz olarak açık kaynak desteği sunan platformlar da bulunmaktadır. Bu proje çalışmasının amacı öncelikle kurumsal ağlarda bilgi toplama yöntemlerini uygulamak, saldırı 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: siber güvenlik, bilgi toplama, ağ saldırısı, saldırı tespiti

ÖNSÖZ

Bu bitirme ödevin oluşturulması esnasında içeriği ve yüzlerce ufak ayrıntının birbirleriyle ahenk içerisinde tezde yer almasında önemli katkılarda bulunan, bilgi, birikim ve engin tecrübeleri ile bana yol gösterici ve destek olan, çalışmalarımızı yönlendiren ve bütün içtenliğiyle yardımcı olan Netkent Akdeniz Araştırma ve Bilim Üniversitesi hocalarımıza ve değerli danışmanımız sayın Dr. Burak OLGUN 'a en içten saygılarımızı ve teşekkürlerimizi sunarız.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklama**
GNU/Linux	Özgür yazılım; kullanıcıların yazılımı çalıştırma, kopyalama, dağıtma, inceleme, değiştirme ve geliştirme özgürlüğüne sahip olduğu anlamına gelir. Not Unix
ICMP	Internet Message Access Protocol, Internet Mesaj Erişim Protokolü
TCP	Post Office Protocol, Postane Protokolü 3
IP	Internet Protocol, İnternet Protokolü
DNS	Domain Name System, Alan Adı Sistemi
NS	Name System, Alan Adı Sistemi
SOA	Service Oriented Architecture, Servis Yönelimli Mimari
MX	Mail Exchanger, Posta Değiştirici
SPF	Sender Policiy Framework, Gönderen Politikası Çerçevesi
TXT	DNS kayıt türü, TXT kayıtları tarihsel sıraya göre okunabilir server,network, data center ve diğer hesap bilgileri hakkında bilgi içerir.
SSH	Secure Shell, Güvenlik Kabuğu, kullanıcılara sunucularını internet üzerinden kontrol etmesini ve düzenlemesini sağlayan uzak yönetim protokolüdür.
TELNET	Internet ağı üzerindeki çok kullanıcılı bir makineye uzaktaki başka bir makineden bağlanmak için geliştirilen bir TCP/IP protokolü ve bu işi yapan programlara verilen genel isimdir.
CSV	Virgülle ayrılmış değerler dosyası, değerleri ayırmak için virgül kullanan sınırlandırılmış bir metin dosyasıdır. Dosyanın her satırı bir veri kaydıdır. Her kayıt, virgülle ayrılmış bir veya

	daha fazla alandan oluşur. Alan ayırıcı olarak virgül kullanılması, bu dosya biçiminin adının kaynağıdır
XLS	Excel File, Excel dosyası
XLSX	Excel 20xx versiyon file, Excel 2007 versiyon sonrası excel dosyası
IDS	Intrusion Detection System, Saldırı Tespit Sistemi
IPS	Intrusion Prevent System, Saldırı Tespit ve Karşı Atak Sistemi

TABLOLAR LİSTESİ

Tablo Adı **Sayfa**

ŞEKİLLER LİSTESİ

Şekil Adı **Sayfa**

Şekil Adı **Sayfa**

GİRİŞ

1.1. Tanım

Bilgi teknolojilerinin kullanımının yaygınlaşması ile son zamanlarda dünyada olduğu gibi ülkemizde de siber güvenliğin önemi artmaktadır. Kullanılan donanım ve destekleyici yazılımlar kullanıcıya çeşitli faydalar sağlamakla birlikte yapısı gereği algoritmik eksiklikler ve güvenlik açıklarına da sebep olmaktadır. Bu durum çeşitli kurum ve kuruluşları, bireysel kullanıcıları, kurumsal web sitelerini ve sistemlerini kötü niyetli şahısların (hacker) saldırılarına açık hale getirmektedir.

Bilgi güvenliği bu saldırıları önlemek adına dijital ortamda depolanan bilgilerin güvenliğini sağlamak için yapılan tüm çalışmaları kapsamaktadır. Bu çalışmalardan biri de penetrasyon (sızma) testleridir.

Sızma ve güvenlik testlerinin en önemli adımlarından bir tanesi hedef hakkında bilgi toplamaktır. Bir hedefe yönelik ne kadar fazla bilgi toplanılabilirse hedefi ele geçirme olasılığı da o kadar artmaktadır. Metodolojik olarak öncelikle uygulanması gereken faz bilgi toplama fazıdır. Bu fazda, Internet üzerindeki servislerden bilgi toplama, hedef alan adına ait IP aralığının tespit edilmesi, hedef alan adına ait email adreslerinin bulunması, hedefin kullandığı yazılımların ve işletim sistemlerinin belirlenmesi, hedefin kullandığı güvenlik sistemlerinin analizi, son kullanıcılar yüklü olan antivirüs programlarının tespiti, eğer test bir kurum ya da şirket üzerine uygulanıyorsa telefon numarası, adres bilgisi gibi bilgilerin internet üzerinden nasıl toplanabileceği ile ilgili bilgiler verilecektir.

Penetrasyon testleri uzman kişiler tarafından var olan bilgi sistemi açıklarının kötü niyetli şahıslardan önce tespit edilip gerekli önlemlerin alınması hususunda bir rapor hazırlanması ve ilgili kişilerin bilgilendirilmesi şeklinde gerçekleştirilmektedir. Özellikle ülkemizde penetrasyon testi uzmanları oldukça az sayıdadır ve bu konuda kendilerini geliştirmek isteyen kişilere yönelik yeterli kaynak son yıllarda vermeye başlanmıştır.

Penetrasyon testlerini yapmadan önce ilgili sistemler için bilgi toplanması sistem hakkında uzman bakış açısıyla değerlendirilmesi gerekmektedir.

1.2. Amaç ve Kapsam

Bilgi toplama aşaması olarak ta kabul edilebilen keşif aşaması penetrasyon testinin gerçek anlamda başladığı aşamadır. (Ami ve Hasan, 2012).

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 ve ücretli yazılımlar ile siber güvenlik literatürleri arasında yer alan siber istihbarat ve penetrasyon testlerinde en çok kullanılan aktif ve pasif bilgi toplama araçlarını kullanarak sonuçların elde edilmesi ve farkındalık oluşturmayı amaçlamıştır.

1.3. Materyal ve Metot

Pasif bilgi toplama aşamasında penetrasyon testi uzmanları, hedef ağları ve sistemleri hakkında doğrudan bağlantı kurmadan olabildiğince çok bilgi toplamaya çalışmaktadır. Pasif bilgi toplama aşamasında birçok farklı türde arama işlemi gerçekleştirilmektedir.

Pasif bilgi toplama yöntemlerinde hedef ile direkt olarak iletişime geçmeden Kali Linux'ta yer alan hazır paket araçlardan, internet üzerindeki servisleri ya da web sitelerini kullanarak hedef hakkında bilgi alınmaktadır. Pasif bilgi toplamak için Google, Bing gibi arama motorları, sosyal paylaşım siteleri, whois sorgusu yapan ve port tarayan web siteleri, arama motorları üzerinden email adreslerini tarayan araçlar kullanılmaktadır.

Aktif bilgi toplama yöntemlerinde ise bilgi toplayan kişi hedef ile direkt olarak etkileşim halinde olur. Örneğin pentest yapan kişi hedefe yönelik bir port taraması, kendisi yapıyor ise yani internet üzerinden herhangi bir servis ya da bir site kullanmadan direkt olarak hedef ile kendisi iletişime geçerek yapıyorsa bu aktif taramaya bir örnek olarak verilebilir.

Bu çalışmada pasif bilgi toplama işlemleri için Windows ve VMWare Sanallaştırma kullanılarak Kali Linux üzerinde hedef sistemlere sırasıyla ping, nslookup, whois, reverse whois/ip lookup, zone transfer, mail ve subdomain tespiti, subdomain ve googlehacking yöntemleri uygulanarak sistemlerle ilgili maksimum bilgiye ulaşılmaya çalışılmıştır.

Pasif bilgi toplama işlemi tamamlandıktan sonra gelen aşama aktif bilgi toplama aşamasıdır. Pasif bilgi toplama aşamasıyla keşfedilen ip ve servis bilgileri aktif bilgi toplama aşamasında kullanılarak özel araç ve yöntemlerle tarama işlemi gerçekleştirilmektedir.

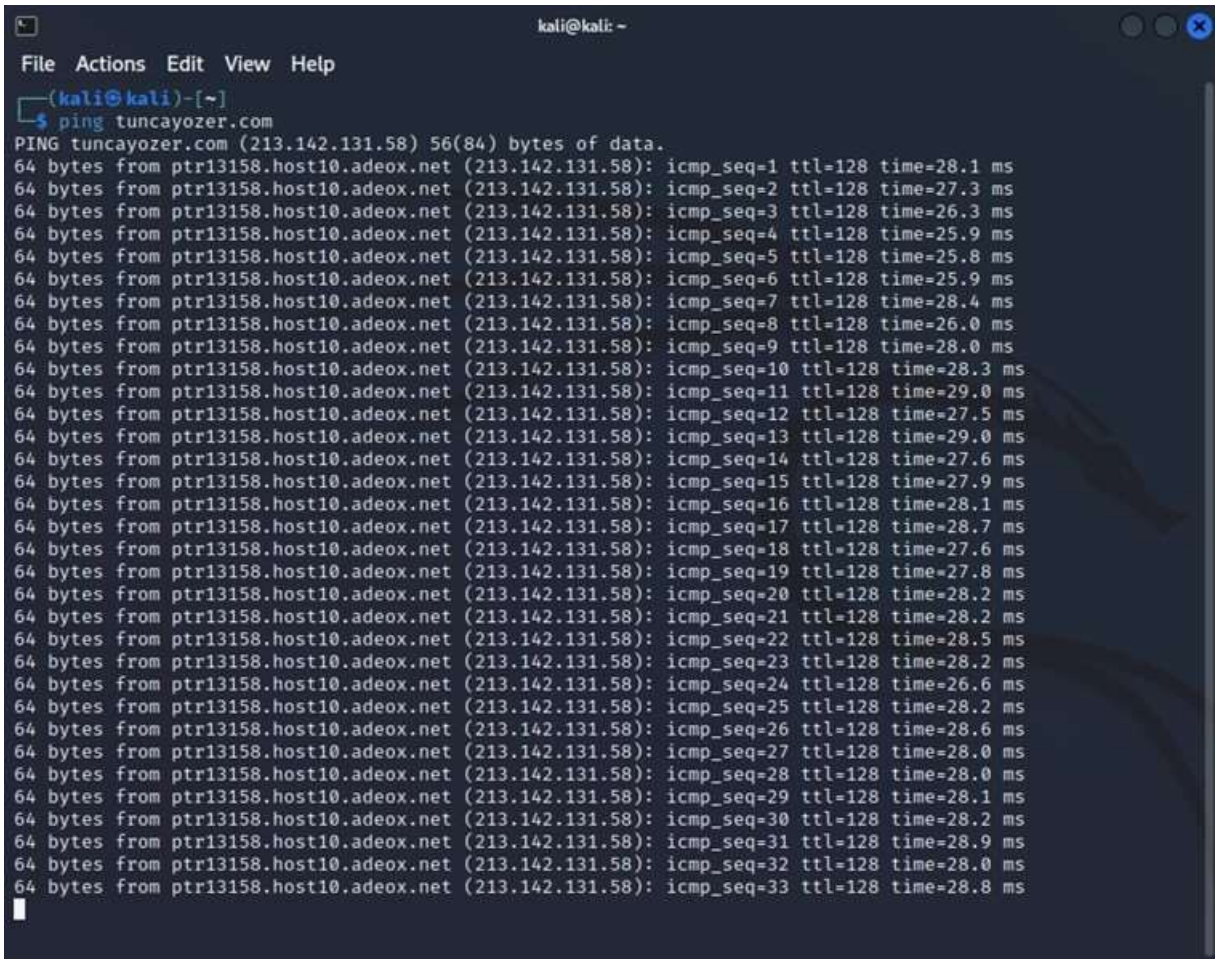
Aktif bilgi toplama aşaması ilgili birimin sistem yöneticileri ya da güvenlik uzmanları tarafından, kurumdaki cihazların log kayıtlarında penetrasyon testi uzmanının yaptığı işlemler görülecek şekilde gerçekleştirilmelidir (Wilhelm, 2010). Bu çalışmada aktif bilgi toplama aracı olarak Nmap yazılımı kullanılarak ağ üzerindeki bir cihazdan işletim sistemi, servis bilgisi, açık port bilgisi gibi bilgilerin toplanması sağlanmıştır.

2. BİLGİ TOPLAMA YÖNTEMLERİ

2.1. Pasif Bilgi Toplama Yöntemleri

2.1.1. Ping Sorgulama

Ping komutu hedef sistem ile iletişimin sağlanıp sağlanmadığını kontrol etmek, hedef sistemle kurulan bağlantı hızını ölçmek ve bir domain alanının işaret ettiği IP adresini tespit etmek için kullanılan bir GNU/Linux ve Microsoft Windows komutudur.

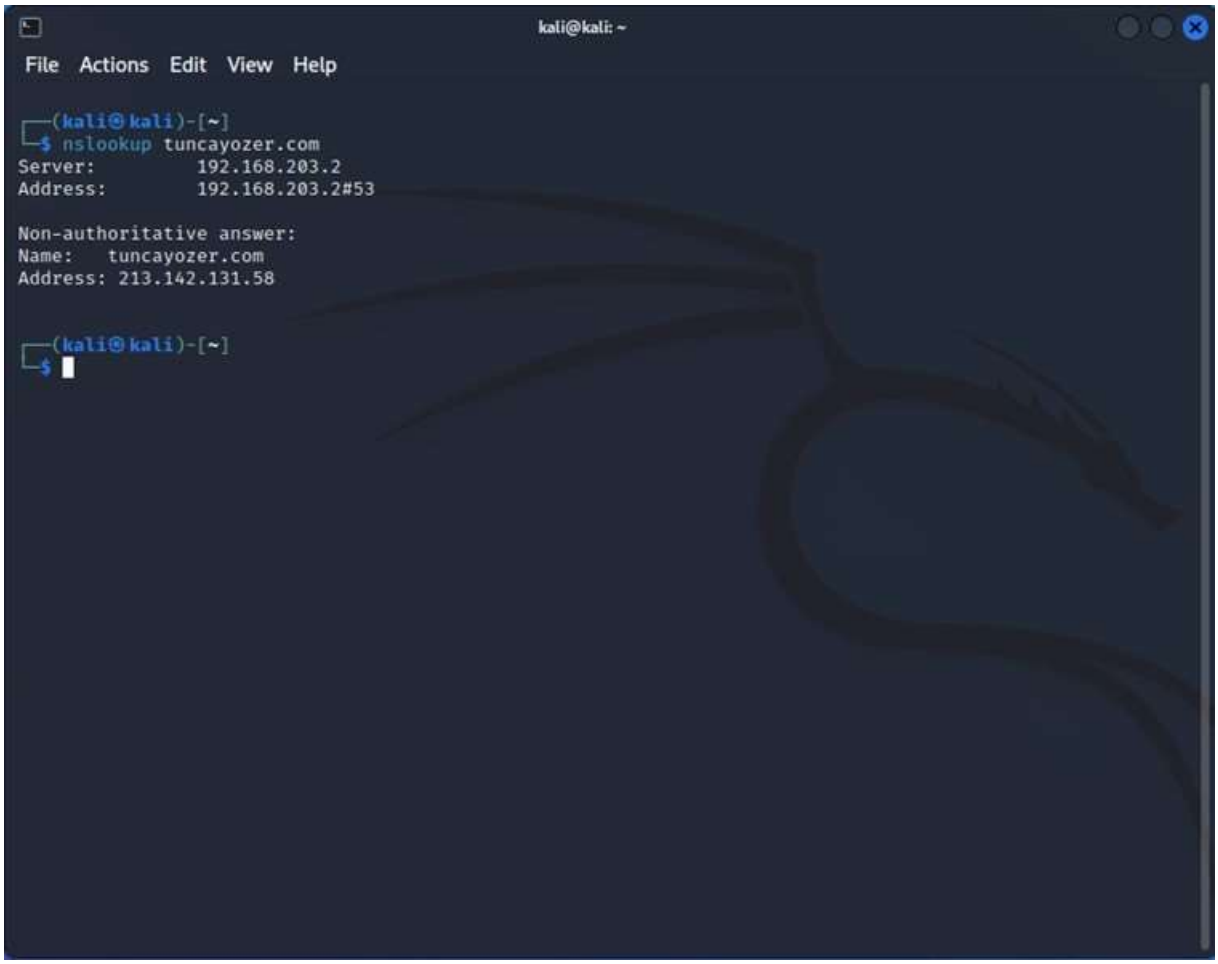


Şekil 2. 1. Ping Komutu.

Şekil 2.1.'de ping komutu ile "google.com" adresine bir ICMP paketi gönderilmiştir. İlgili domainin işaret ettiği IP adresi 213.142.131.58 olarak gösterilmiştir. Ping komutunun cevap alabilmesi hedef makine ile iletişim sağlandığını göstermekte ve iletişim sağlanan makinenin aktif olduğu anlamına gelmektedir. Ping komutunun hedef makineden cevap alamaması direk olarak hedef makinenin çöktüğü anlamına gelmez. Microsoft cihazlarında güvenlik duvarı varsayılan olarak açıktır ve ICMP paketlerini engellemektedir. Bu durum da ping komutunun hedef makineden cevap alamamasına sebep olmaktadır.

2.1.2. Nslookup Sorgulama

Nslookup domain alanlarının işaret ettiği IP adreslerini çözümlemek için kullanılan bir script'tir. Ping komutu domain alanlarının işaret ettiği ip adresleri gösterirken aynı zamanda hedef makine ile iletişimin sağlanıp sağlanamadığı, iletişim hızı gibi bilgileri de sunmaktadır. Fakat nslookup yalnızca domain alanlarının işaret ettiği ip adreslerini çözümlemek amacıyla kullanılmaktadır.



Şekil 2. 2. Nslookup komutu

Şekil 2.2.'de nslookup script'i kullanılarak tuncayozer.com domain alanının işaret ettiği IP adresi bilgisine ulaşılmıştır.

2.1.3. Host Sorgulama

Host komutu bir domain alanının işaret ettiği IP adresini ve bir IP adresinin sahip olduğu domain alanını göstermek için kullanılan bir komuttur. Host komutunun çeşitli kullanım şekilleri mevcuttur fakat bu çalışma kapsamında yalnızca bu iki özelliği kullanılmıştır.

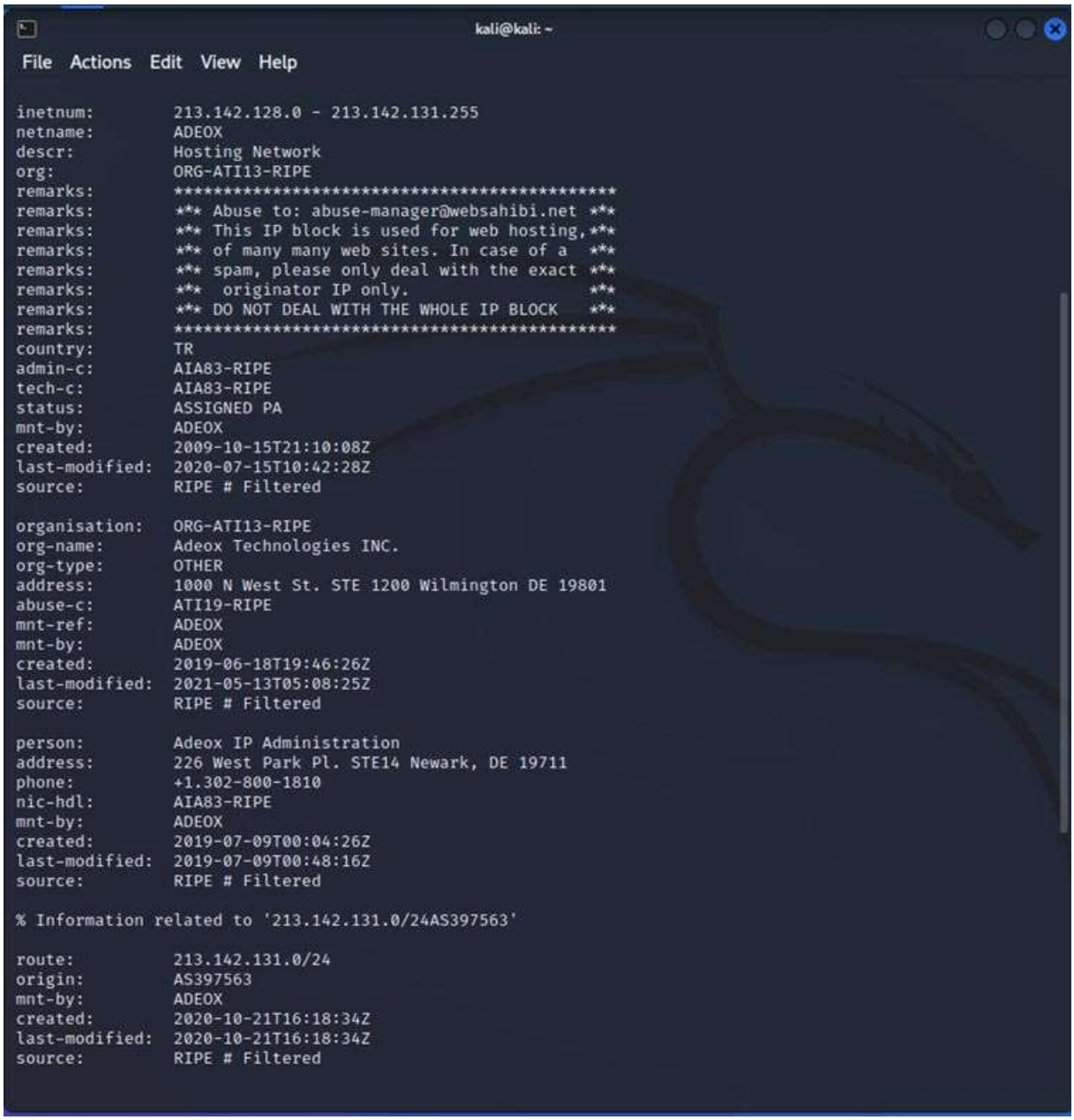
Şekil 2. 3.Host komutu

Şekil 2.3.'te host komutu kullanılarak tuncayozer.com domain alanının IP adres bilgilerine ve IP adresi kullanıldığında domain alanı adına erişim sağlanmıştır. Mail servisi olarak da mail.yandex.net adres olarak görünmüştür. Linux üzerinde bir bash scripting kullanılarak bir domain, subnet veya IP listesindeki domainlerin tespiti için host komutu kullanılabilmektedir.

2.1.4. Whois Sorgulama

Whois bir domain veya bir IP 'nin sahiplik bilgilerinin öğrenildiği bir sorgu komutudur. Whois eski bir sorgu komutudur ve yalnızca Kali Linux'a ait değildir. Domain firmalarından domain veya sunucu satın alınırken iletişim bilgileri de dahil olmak üzere verilen müşteri bilgileri bazı firmalar tarafından ücretsiz olarak gizli hale getirilirken bazı firmalar bu işlemi belirli bir ücret karşılığında gerçekleştirmektedir. Whois sorgu komutu domain veya sunucu satın alınırken verilen bilgilerin gizli hale getirilmemesinden dolayı bu bilgilere erişim sağlayabilmektedir. Bu bilgilere erişim internet üzerinden de gerçekleştirilebilir fakat Kali Linux üzerinde bu işlemi gerçekleştirmek için bir whois yazılımı mevcuttur. "tuncayozer.com" komutu kullanıldığında çıkan sonuç Şekil 2.4. ve 2.5.'de gösterilmektedir.

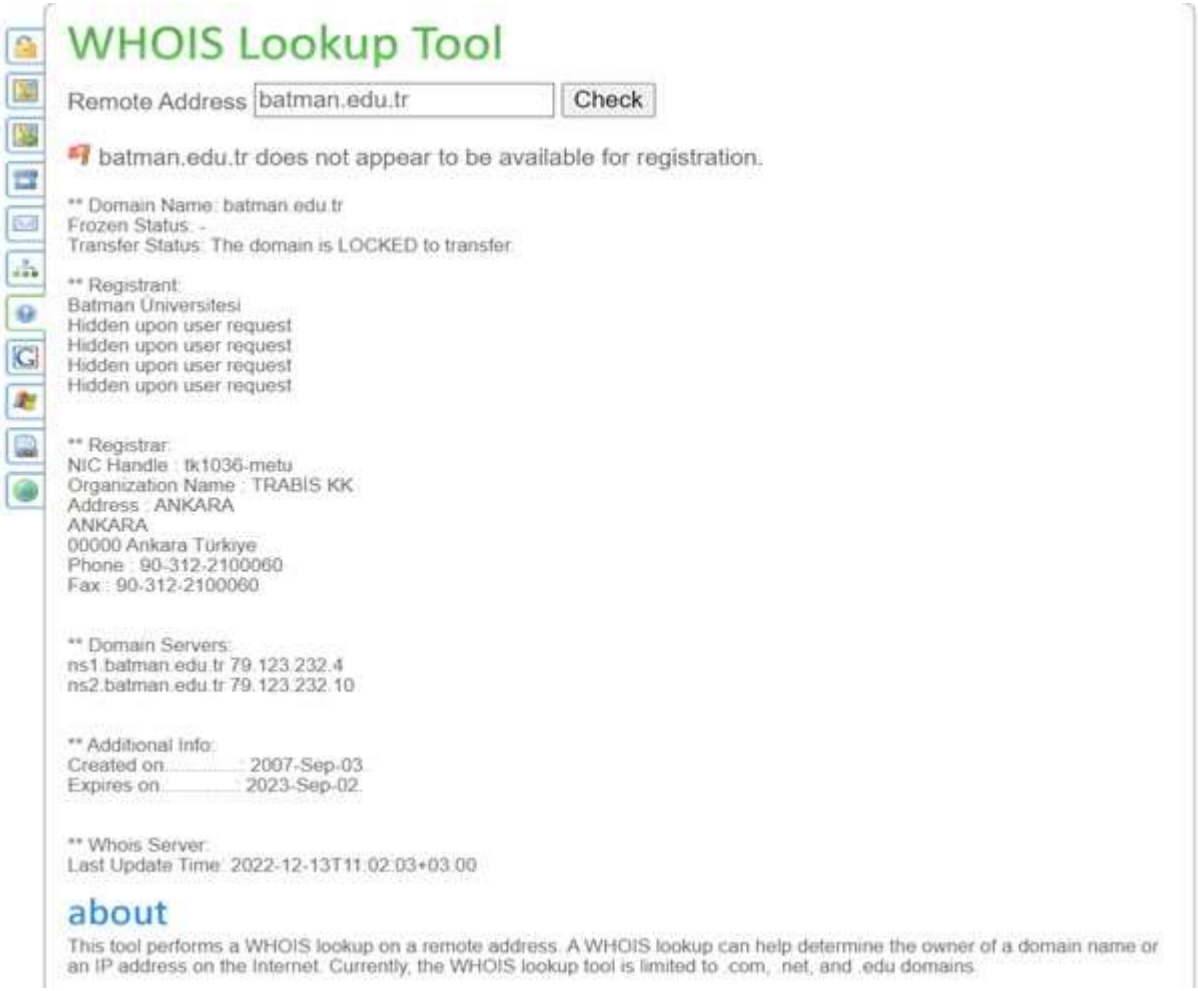
Şekil 2. 4.Whois komutu



Şekil 2. 5.Whois Ip

2.1.5. Reverse Whois/IP Lookup

Reverse Whois veya IP Lookup, herhangi bir IP üzerinde bulunan domainlerin ve IP ile ilgili mümkün olduğunca fazla bilginin tespitini sağlamak için kullanılan bir tarama aracıdır. Bu bölümde ip lookup işlemi bir internet uygulaması kullanılarak sunulmuştur. Fakat reverse whois IP lookup işlemleri google hacking bilgi toplama yönteminde de uygulanacaktır. Bu bölümde kullanılacak site “you get signal reverse ip lookup” tır.



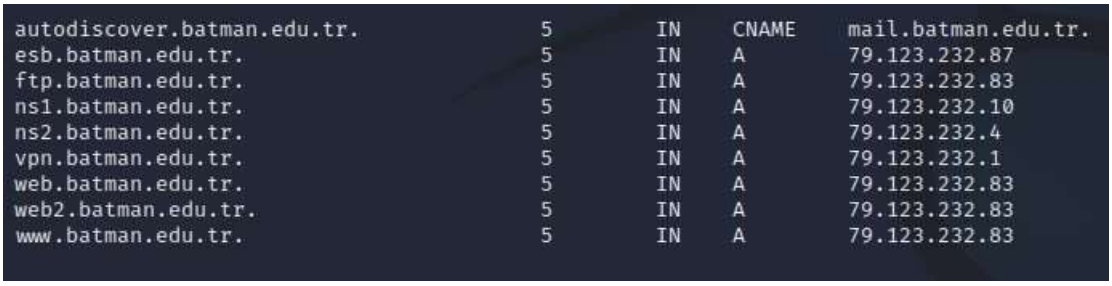
Şekil 2. 6. Reverse Whois Lookup

Şekil 2. 7. Reverse Ip Domain Check

Şekil 2.7.'de yougetsignal.com sitesine herhangi bir domain veya IP adresi girilebilmektedir. Eğer domain adresi girilirse IP adresine çözümler ve bu IP adresine bağlı sunucuları getirmektedir. Bu yöntem elde edilen subnet üzerindeki dışa açık IP'lere bağlı web sitelerin bulunmasında sık kullanılan bir yöntemdir. Şekil 2.7.'de batman.edu.tr domain adı girildiğinde sonuç olarak bu domainin IP adresine bağlı sunucuları getirecektir. Aynı görselde görülen ilgili IP adresi taranarak sonucun doğruluğu kontrol edilebilmektedir.

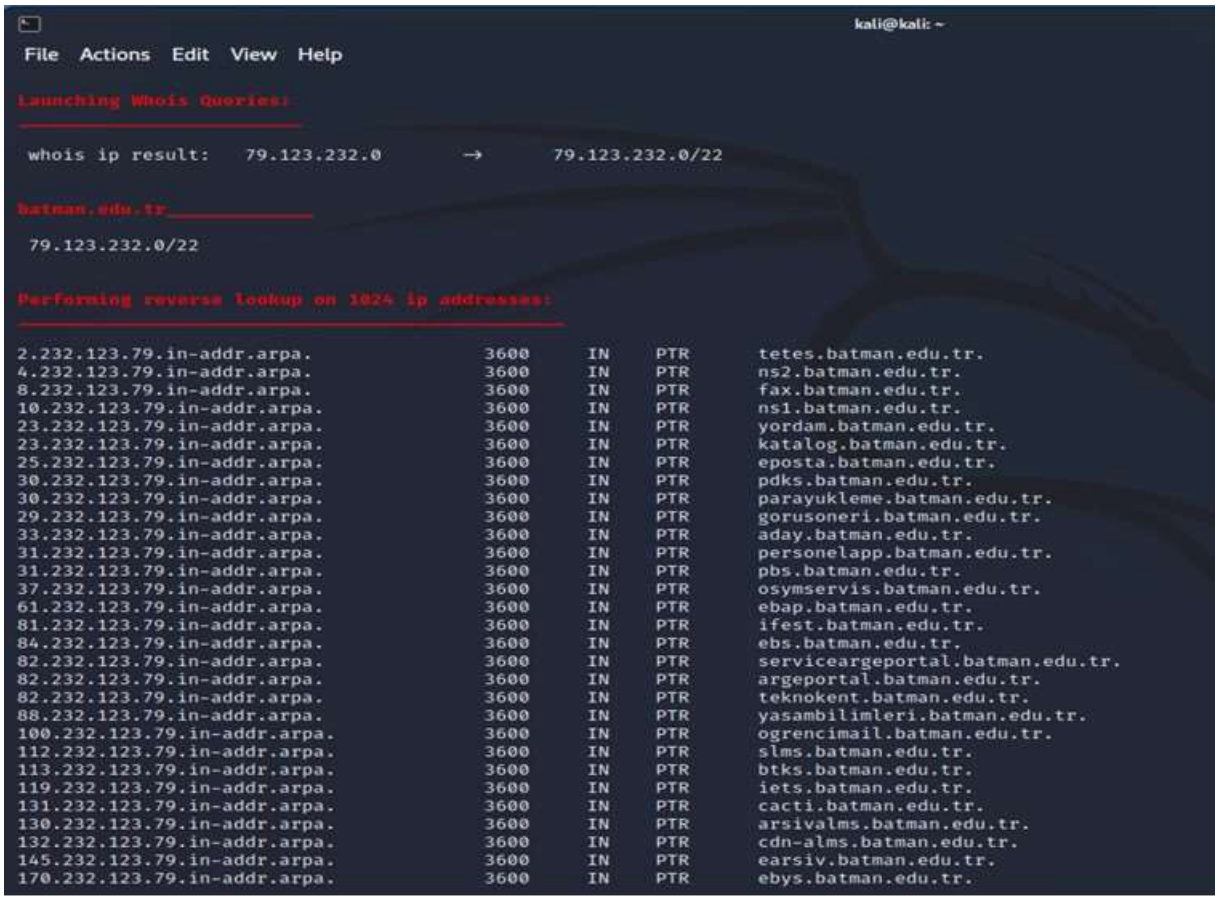
2.1.6. Subdomain ve Mail Tespiti

Hedef sistemin subdomain ve mail adresi tespitleri daha önceden sunulmuş The Harvester aracı kullanılarak pasif bilgi toplama yöntemleri altında incelenebilmektedir. The Harvester aracı farklı arama motorları üzerine sorgular yollayarak dönen cevapları ayıklar ve istenilen sonucu döndürür. Bu sonuçların içerisinde ilgili domain adına paylaşılmış mail ve subdomain bilgileri yer almaktadır.



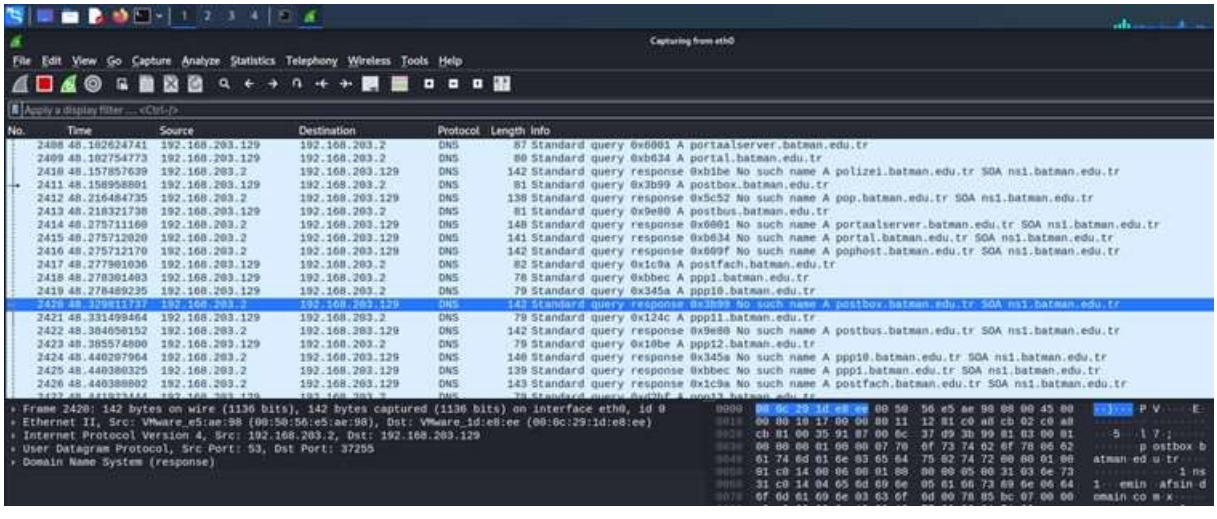
Şekil 2. 8. Subdomain bilgileri

Şekil 2.8.'de Theharvester aracı ile microsoft.com domaini ile biten mail ve subdomainlerin arama işlemi gerçekleştirilmiştir. Elde edilen sonuçların bir kesiti Şekil 2.9.'daki gibidir.



Şekil 2. 9. Theharvester Komutu Sonucu Bilgi Kesiti

Görüldüğü üzere yaklaşık 16 tane subdomain adresi bulunmuştur. Fakat herhangi bir mail adresine ulaşılamamıştır. Arama sonucu elde edilen subdomain ve mail adresleri sosyal mühendislik saldırıları ve tarama işlemlerinde kullanılabilmektedir. Arka planda Theharvester aracının gönderdiği istekler wireshark aracı ile ayrıntılı bir şekilde gözlemlenebilmektedir.

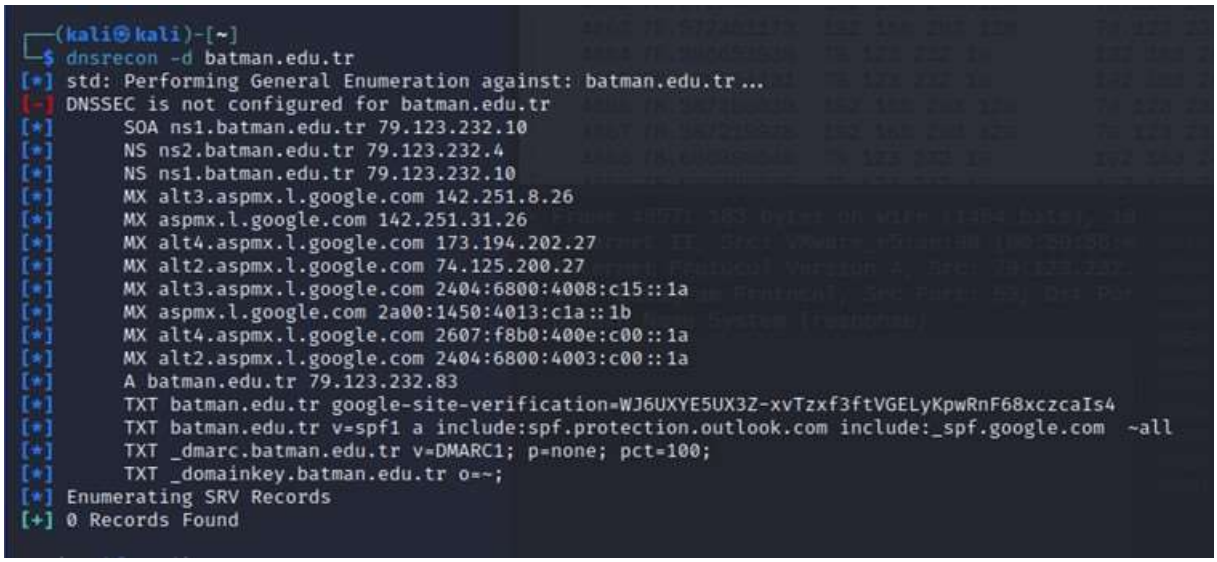


Şekil 2. 10. Theharvester komutu Wireshark dinlemesi

Şekil 2.10.'de wireshark'ta görüntülenen ara yüzlerden eth0 dinlemeye alınmıştır ve Theharvester tekrar çalıştırılmıştır. Theharvester tekrar çalışmaya başladığında wireshark üzerinde birden çok istek görülmüştür.

2.1.7. SubDomain

Bu bölümde daha detaylı bir domain saptaması gerçekleştirmek için dnsrecon aracı kullanılmıştır.



Şekil 2. 11. DNSrecon aracı

Şekil 2.11.'de Kali Linux ilk olarak zone transferleri kontrol eder ve zone transferler üzerindeki subdomainleri tespit etmektedir. Tarama ile bizlere SOA, NS, TXT, SVR, SPF vb. gibi DNS kayıtlarını getirir. Belirli bir etki alanı için DNS kayıtlarını numaralandırma işlemi burada gerçekleşmektedir.

SOA (Start of Autority): Zone transferi DNS veritabanının bir sunucudan başka bir sunucuya aktarılması işlemidir. SOA ise Bulunduğu DNS Server üzerinde zone transferinden sorumlu olduğunu belirleyen kayıttır.

MX (Mail Exchange): Alan adınıza gelen e-posta iletilerinin hangi sunucuya yönlendirilmesi gerektiğini gösteren kayıt tipidir.

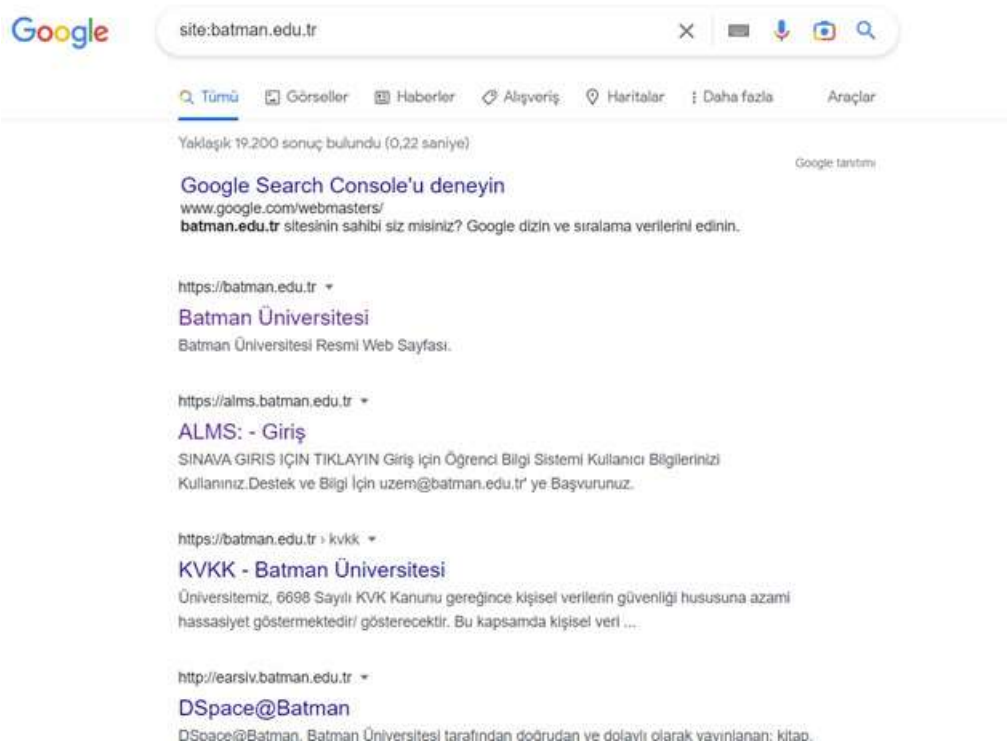
NS (Name Server): Network üzerinde bulunan DNS Server'ları tanımlar. Bu kayıt sayesinde bir DNS Server diğer DNS Server ile network aracılığıyla iletişime geçebilir.

SPF (Sender Policy Framework): SPF kaydı, hangi posta sunucuları tarafından alan adınıza e-posta gönderilmesini denetleyen kayıtları içerir.

2.1.8. Google Hacking

Bu bölümde ilgili işlemler için internet tarayacısı üzerinde bulunan google ve bing arama motorları kullanılmıştır. Bu arama motorlarının hepsinin çalışma mantığı basit olmakla

birlikte aynıdır. Hepsi özel aramalar (dorglar) aracılığı ile arama motorlarının indekslediği bilgileri kullanıcıya sunmaktadır. Google üzerinde arama yapmak için kullanılan başlıca dorglar site, inurl, intext, filetype dorglarıdır. Bing üzerinde arama yapmak için kullanılan en bilindik dorg ise ip dorg'udur. Bing bu ip üzerinde indeksleyebildiği tüm bilgileri sunmaktadır. Bu aramalar sayesinde arama motorları belirli bir domaine ait subdomain tespitlerini gerçekleştirmektedir.



Şekil 2. 12. Google Araması

Ayrıca google aramasında kullanılabilecek yöntemlerde mevcuttur. Bunlar;

inurl: belirtilen sözcüğü URL adreslerinde arama yapar.

Filetype: ilgili dosya uzantısında arama yapar.

intitle : belirtilen ifadeyi başlıklarda ara.

Allintittle: belirtilen ifadeleri başlıkta arar.

Gibi önek Google komutları yer almaktadır.

2.1.9. Shodan

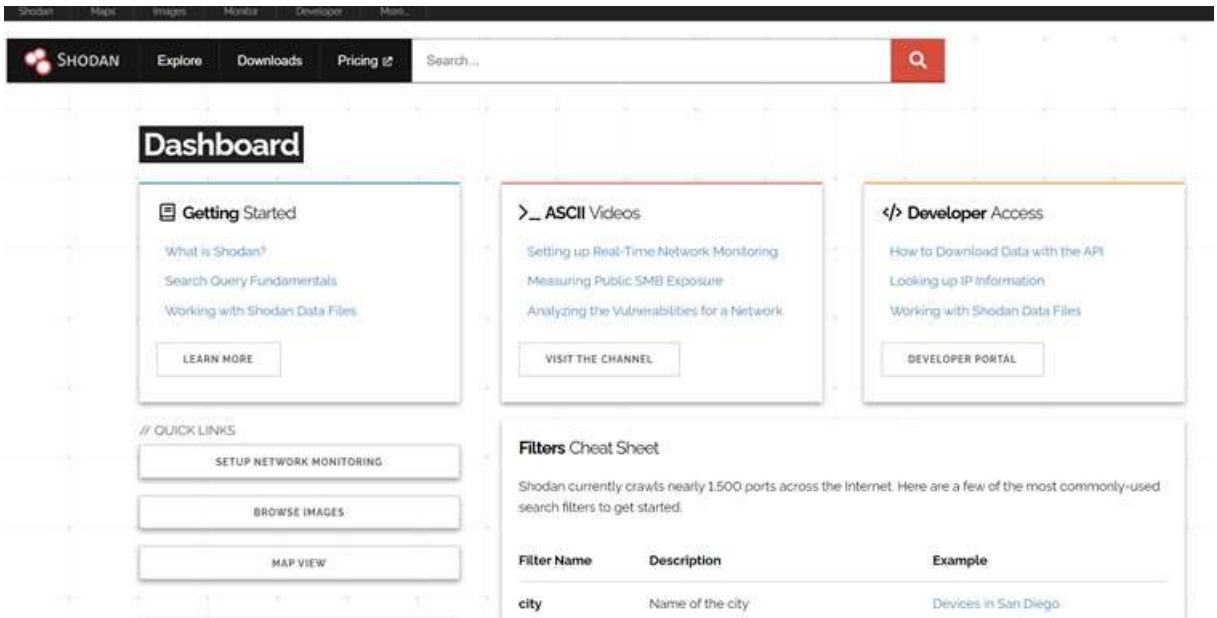
Shodan, belirli filtreler kullanarak, belirli coğrafi bölgelerde işlev gören bilgisayar sistemlerindeki açık portları, çalışan servisleri, varsayılan parolaları, ağ cihazlarını

arayabileceğiniz bir arama motoru olarak kullanabileceğiniz web tabanlı bir araçtır. Shodan'a http://www.shodan.io adresinden ulaşabilirsiniz.

Shodan (Sentient Hyper-Optimized Data Access Network), internete açık olan gizli kameralar, SSH sunucuları, web uygulamaları, yönlendirici veya güvenlik duvarı gibi ağ cihazları, SCADA sistemleri gibi birçok sistem üzerinden bilgi elde etme amaçlı kullanılan özelleştirilmiş arama motoru, analiz aracı, görselleştirme uygulaması ve çok daha fazlasıdır.

Shodan.io adresinden gerekli ücretli-ücretsiz üyelik işlemi yapıldıktan sonra çeşitli işlemler yapılmaktadır. (shodan.io) Shodan'da kullanabileceğiniz, aratabileceğiniz pek çok unsur bulunmaktadır. Bu unsurları gerek ücretsiz gerek de ücretli bir şekilde kullanabilmekle beraber Shodan üzerinden bir hesap açarak da bu unsurları kullanabilirsiniz. Shodan'ı etkili bir şekilde kullanmak istiyorsanız üyelik ücretiyle kullanmanız daha mantıklı olacaktır. Shodan kullanarak aşağıda çeşitli işlemler yapabilirsiniz. Şekil 2.13.

- Arama Kutusu: Yapacağınız arama kriterleri bu alana yazabilirsiniz.
- Ülke Haritası: Harita üzerinden yapacağınız taramanın sonucunu kapsayacak ülkeyi veya ülkeleri seçebilirsiniz.
- Servis Filtreleme: Yaptığınız aramanın hangi servisleri içereceğini seçebilirsiniz.
- Seçenekler Sekmesi: Tarama sonucunun analizinde ve kriterleri gözden geçirmede detaylı bilgi alabileceğiniz yerdir.



Şekil 2. 13. Shodan Ekranı

Shodan ile birçok bilgiye erişebilirken belirli filtreleri bilmek bilgilere erişmeyi kolaylaştırır. Aşağıdaki filtrelere göre aramalarını daraltabilir veya genişletebilirsiniz:

country: Belirtilen ülke kodunda arama yapar.

city: Belirtilen şehirde filtreleme yapar.

geo: Koordinatlarda arama yapar.

hostname: Hostname yada domain bilgisine göre filtreleme yapar.

net: Özel IP yada subnet aralığında filtreleme yapar.

os: İşletim sistemine göre filtreleme yapar.

port: Port bilgisine göre filtreleme yapar.

before/after: Belirtilen tarih öncesi yada sonrasında yapılan taramaları filtreler.

org: Bellirtilen IP'nin sahibi olan kuruluşa göre filtreleme yapar.

product: Belirtilen ürüne göre filtreleme yapar. Örn: (ApacheTomcat/Coyote JSP engine)

version: Belirtilen versiyona göre filtreleme yapar.

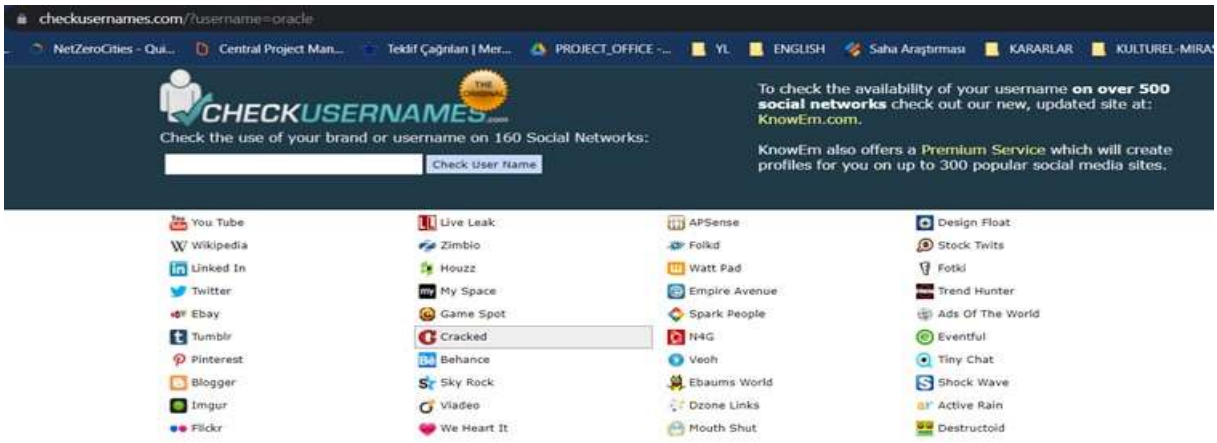
Not: ":" 'dan sonra boşluk bırakılmamalıdır.

Söz ettiğimiz özellik ve filtrelerle birlikte Shodan üzerinden çeşitli taramalar yapmaktadır.

2.1.10. Checkusernames

Yüzlerce sosyal ağ arasında kişi, marka, kullanıcı adı gibi daha önce alınana kullanıcıların sosyal ağ üzerinde hangilerinde kayıtlı olduğunu görmenize yarayan bir sorgulama sitesidir. Şekil 2.14. Ayrıca aynı işlemleri yapan aşağıda belirtilen web siteleri de mevcuttur.

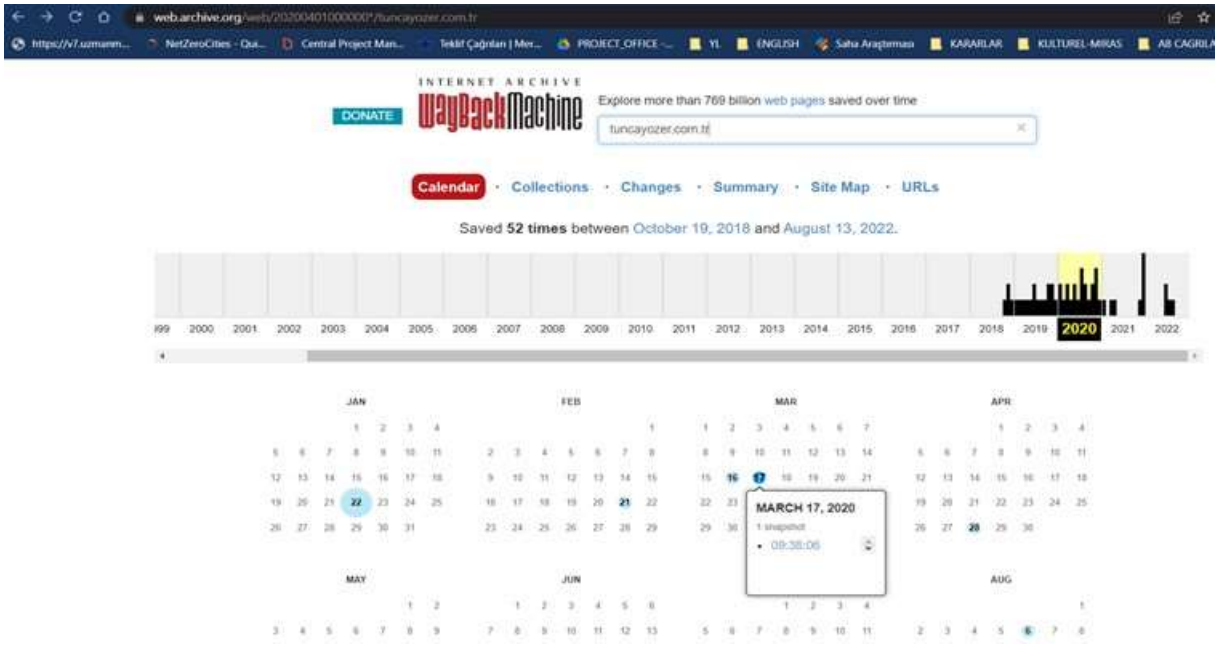
- https://namechk.com/
- https://www.namecheckr.com/
- https://knowem.com/



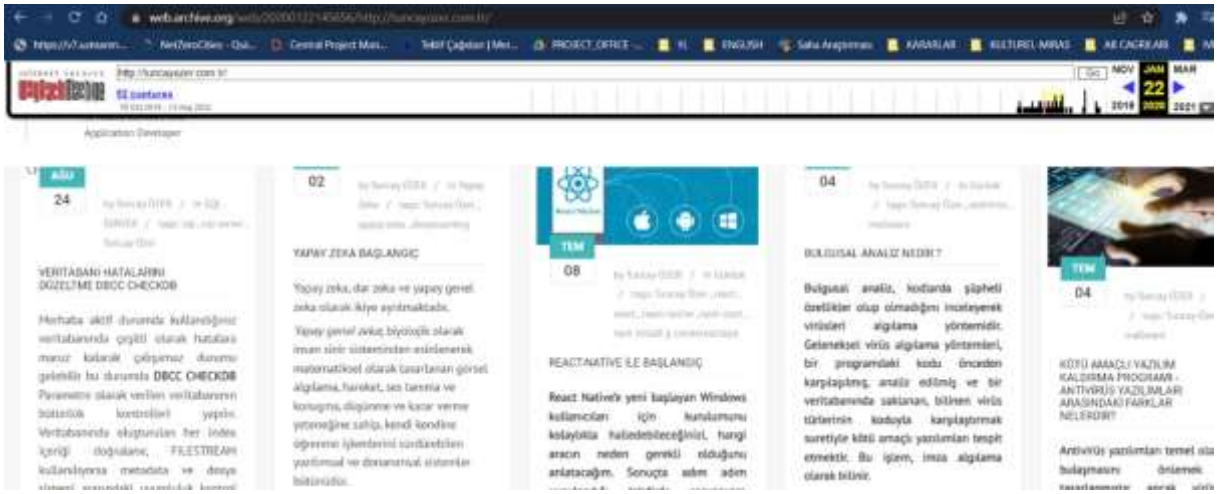
Şekil 2. 14. Checkusername Ekranı

2.1.11. Web Arşivi Sorgulama

Bir web sitesinin geçmiş kayıtlarına bakaraktan hangi işlemlerin veya web sitesindeki değişiklikleri görmemize yarayan bir web sitesi hizmetidir(archive.org). Örnek olarak tuncayozer.com.tr araması yapılmış, sonuçlar Şekil 2.15. ve Şekil 2.16. 'da verilmiştir.



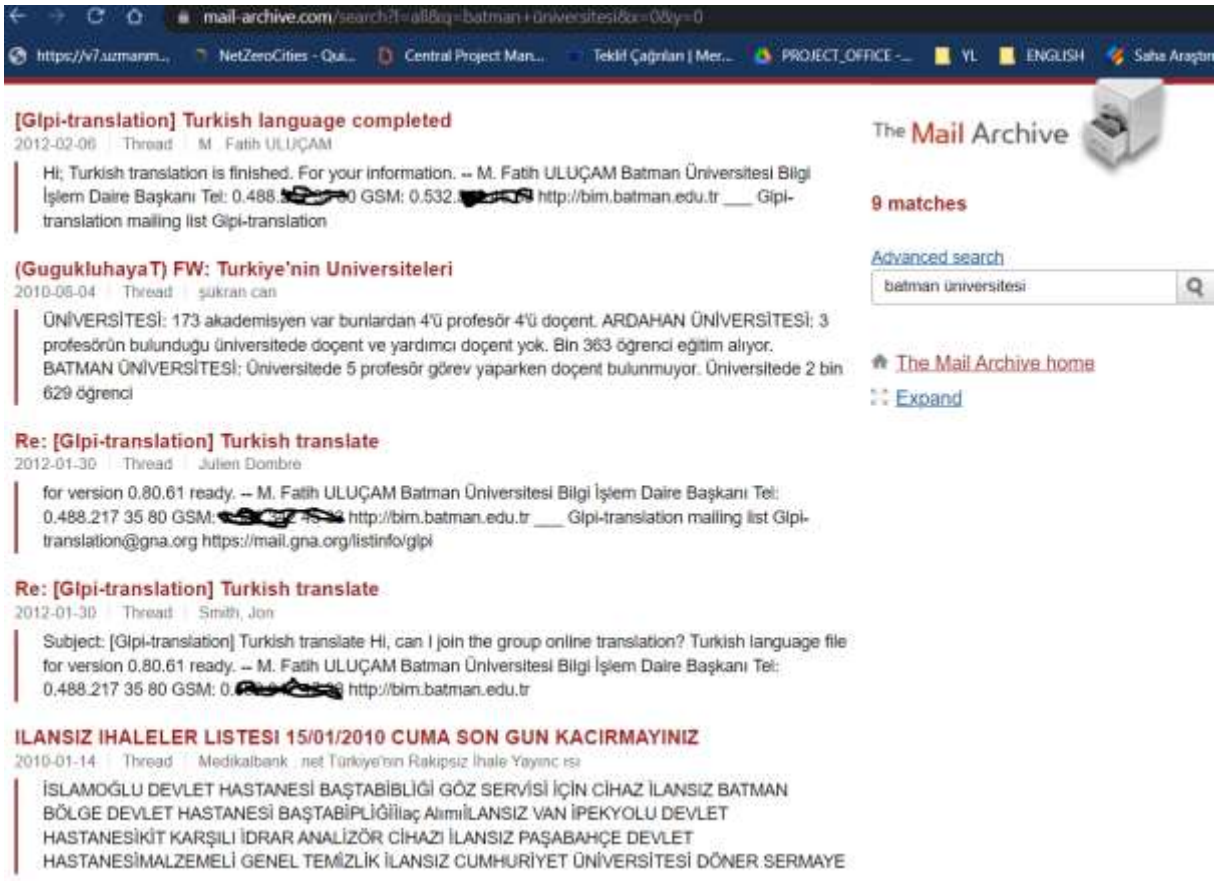
Şekil 2. 15. archive.org web arşivi sorgulama



Şekil 2. 16. Archive.org tuncayozer.com.tr sorgulama sonucu

2.1.12. Mail Arşivi

Bu web sitesinin vermiş olduğu hizmet de e-mail gruplarında yer alan, arşivlenmiş maillerde arama yapmanızı sağlar. (https://mail-archive.com) Şekil 2.17.

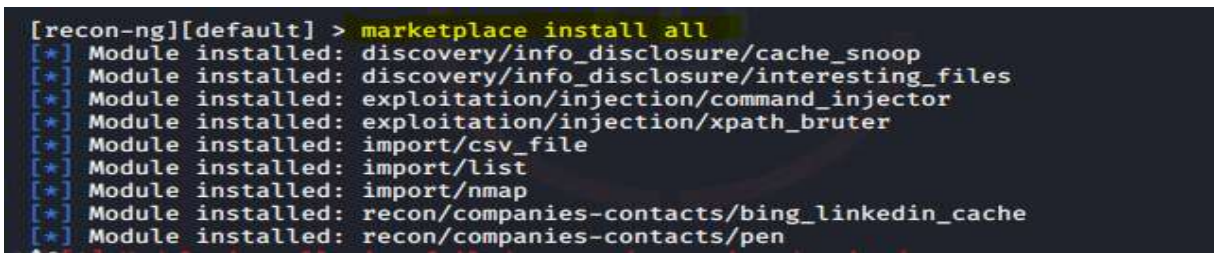


Şekil 2. 17. Mail arşivi sorgulama sonuçları

2.1.13. Recon-ng

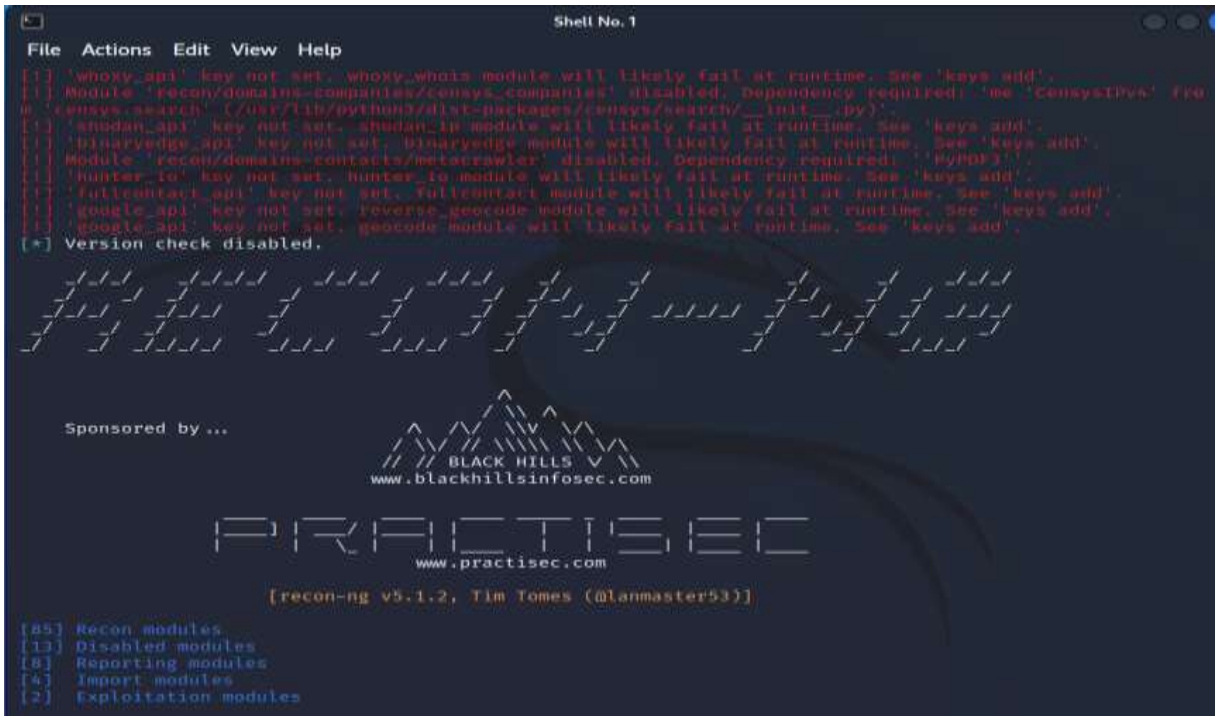
Recon-ng, Python'da yazılmış tam özellikli bir Web Keşif çerçevesidir. Bağımsız modüller, veritabanı etkileşimi, yerleşik kolaylık işlevleri, etkileşimli yardım ve komut tamamlama ile tamamlanan Recon-ng, açık kaynaklı web tabanlı keşiflerin hızlı ve kapsamlı bir şekilde yürütülebileceği güçlü bir ortam sağlar.

Recon-ng aracında 100 civarında modül var ama modüller kurulu olarak gelmiyor. Tek satırlık kodla modüllerin hepsi kurulabilir. Tüm modülleri kurmak için (marketplace install all) komutu kullanılmaktadır. Kullanılan Kali 2022.4 versiyonunda modüller yer almamaktadır. Şekil 2.18'de kurulumu verilmiştir.



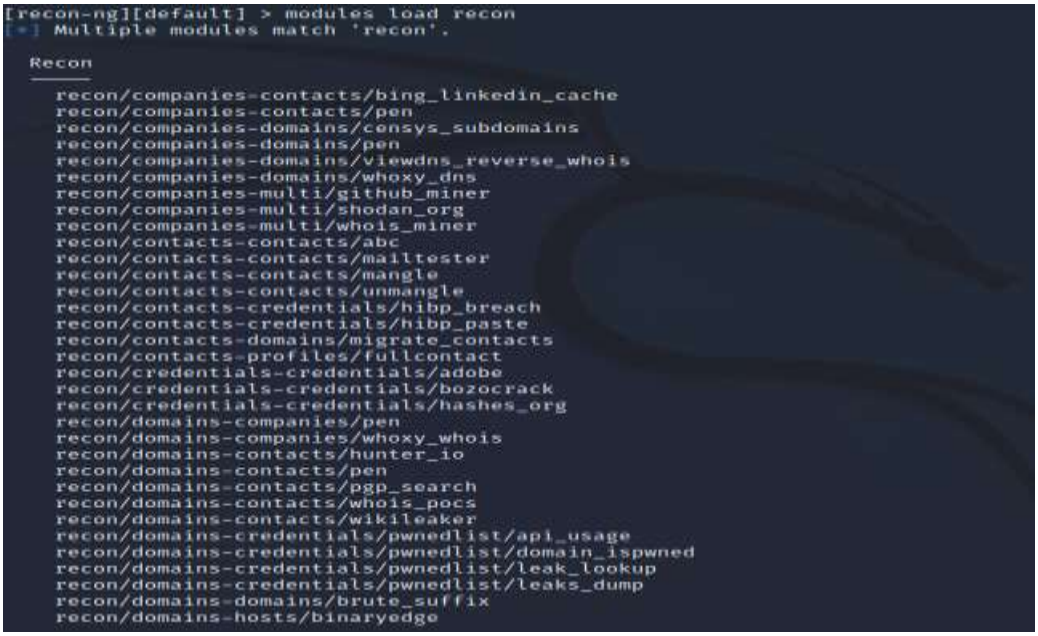
Şekil 2. 18. Recon-ng modül kurulumu

Recon-ng aracındaki modülleri kullanmak API gerektirir. Modüller kurulduktan sonra api bilgisi girilmeyen modüller açılışta kırmızı yazılı uyarı verir. Şekil 2.19.



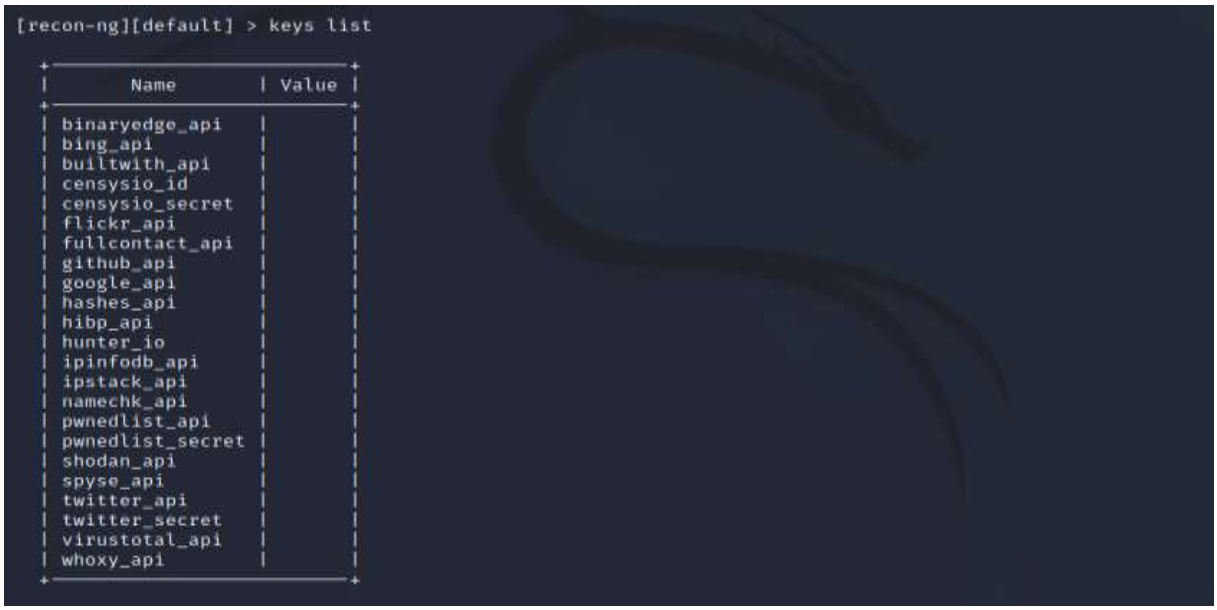
Şekil 2. 19. Modül Uyarıları

Araçtaki modülleri listelemek için (modules search) komutu kullanılır. Ekran resminde bir kısım modüller görüntülenmektedir. Şekil 2.20. Modül hakkında detaylı bilgi almak için(info) komutu kullanılır.



Şekil 2. 20. Modül Listeleme

Modülün çalışması için eklenmesi gereken bilgiler Options: bölümünde yer alır. Bilgileri modüle eklemek için (options set SOURCE) parametreleri kullanılır. Ayrıca modülleri kullanmak için ilgili modül üreticilerinin API keyine ihtiyacı vardır. Bunu liste halinde görebilmek için (keys list) komutu çalıştırılır. Şekil 2.21.



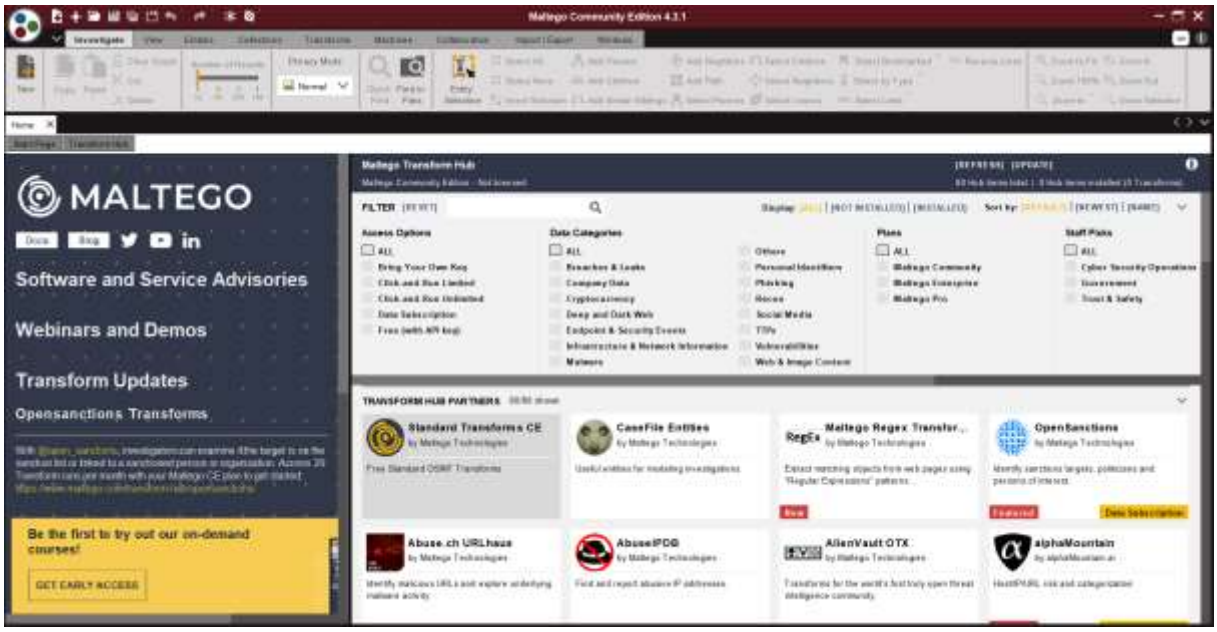
Şekil 2. 21. API Key ihtiyacı olan modüller listesi

2.1.14. Maltego

Maltego (maltego.com), bilgi toplama araçları arasında en ayrıntılı ve kapsamlı bilgiyi sunmasıyla öne çıkmaktadır. Maltego ile hedef sistem hakkında bilgi toplamakla beraber kişiler, kurumlar ve organizasyonlar hakkında da bilgi toplanabilmektedir. Maltego ile hedeflenen sistemin alan adı etki alanları, IP adresleri, DNS kayıtları, telefon numaraları gibi birçok önemli bilgiye ulaşabilmektedir. Maltego, Paterva firmasının ticari bir ürünüdür, fakat ücretsiz ve kısıtlı özellikleri olan sürümü de Kali Linux'ta yer almaktadır. Ayrıca ürünün resmi web sitesinden diğer işletim sistemleri için de indirilebilir sürümleri bulunmaktadır. Maltego'yu kullanmak için kayıt olmanız gerekmektedir. Maltego'nun birkaç özellikleri aşağıda belirtilmiştir.

- Tek bir grafikte 10.000'e kadar Varlık üzerinde bağlantı analizi yapabilme.
- Dönüşüm başına 12 adede kadar sonuç döndürme yeteneği.
- Ortak özelliklere sahip varlıkları otomatik olarak gruplayan koleksiyon düğümlerinin dahil edilmesi.
- Tek bir oturumda birden fazla analistle grafikleri gerçek zamanlı olarak paylaşın.
- Aşağıdakiler dahil grafik dışa aktarma seçenekleri: Görüntüler (jpg, bmp ve png), Raporlar (PDF), Tablo biçimleri (csv, xls ve xlsx), GraphML ve varlık listeleri.

- Aşağıdakiler dahil grafik içe aktarma seçenekleri: Tablo biçimleri (csv, xls ve xlsx) ve grafik kopyalama ve yapıştırma özellikleri.



Şekil 2. 22. Maltego

2.1.15. Zone Transfer

DNS sunuculan yapılandırılırken DNSSEC uygulanmaması ya da eksik güvenlik yapılandırılmalarından kaynaklanan açıklardan dolayı DNS üzerinde var olan kayıtlar transfer edilebilmektedir. Bu kayıtlarda hedef hakkında çeşitli bilgiler vardır. Örneğin DNS kayıtlarında yer alan A kayıtları MX,NS kayıtları, alt alan adları, IP adres bilgileri gibi önemli bilgiler DNS Zone transfer ile elde edilebilir. Örneğin Kali Linux'ta fierce aracı kullanılarak http://zonetransfer.me adlı web sitesinden zone transfer yapılabilir.

```
root@blackbox:~# fierce -dns zonetransfer.me -range
Option range requires an argument
DNS Servers for zonetransfer.me:
        nsztm1.digi.ninja
        nsztm2.digi.ninja

Trying zone transfer first...
        Testing nsztm1.digi.ninja

Whoah, it worked - misconfigured DNS server found:
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ni
nja. (
                                        2014101601      ; Serial
                                        172800  ; Refresh
                                        900     ; Retry
                                        1209600 ; Expire
                                        3600 )  ; Minimum TTL
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J
7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      A       217.147.180.162
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
```

Şekil 2. 23. DNS Zone Transfer

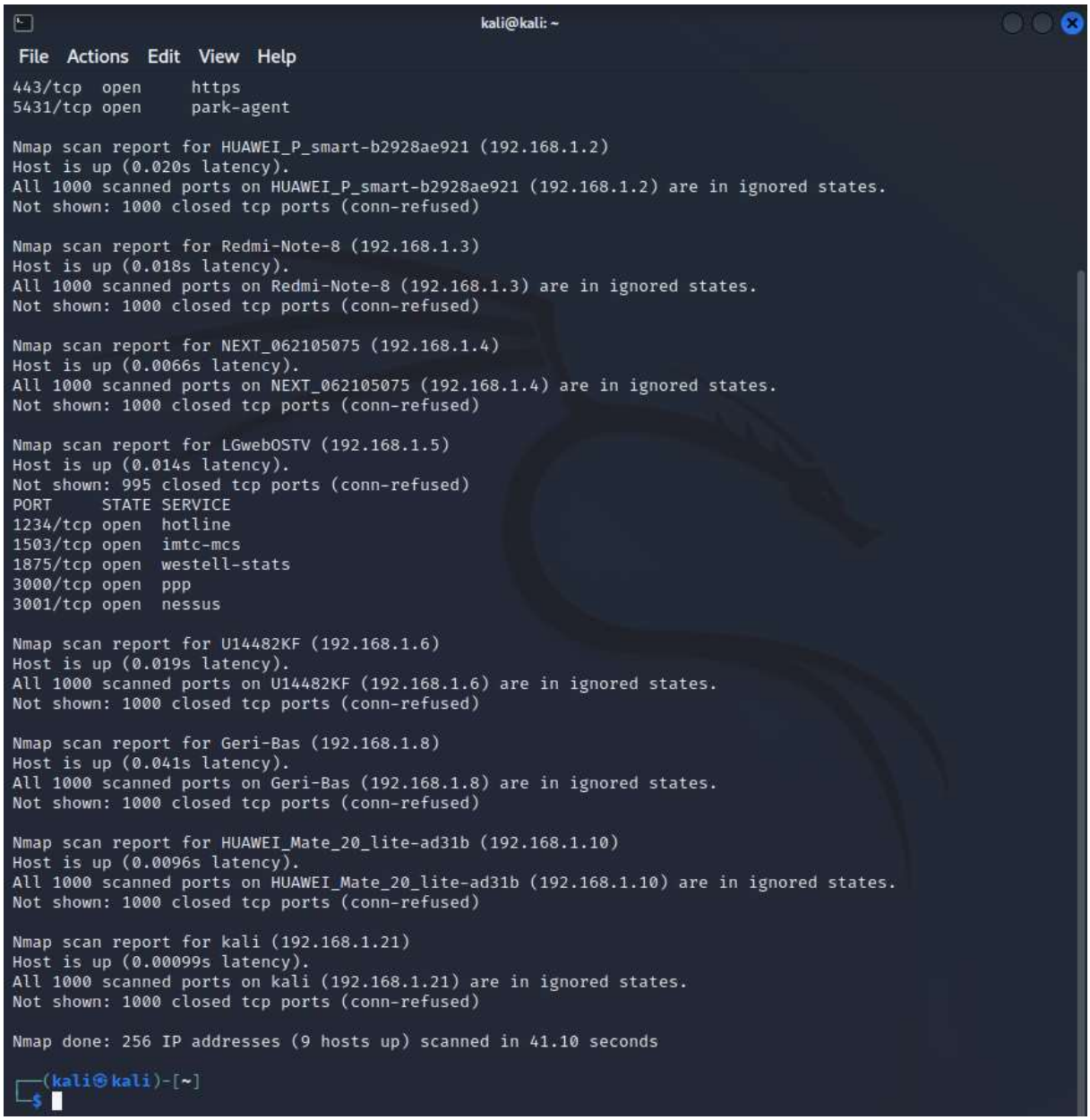
2.2. Aktif Bilgi Toplama Yöntemleri

2.2.1. Ağ Üzerindeki Cihazların Tespit Edilmesi

Bu bölümde nmap yazılımı kullanılarak aynı subnet üzerinde olan cihaz yazılımlarının tespit edilmesi işlemi gerçekleştirilmiştir. Nmap yazılımı Linux ve Windows tabanlı işletim sistemlerinde kullanılabilmektedir. Windows işletim sistemi için üreticinin kendi web sitesinden nmap yazılımı indirilerek kullanılır. Kali Linux'ta kurulu olarak gelmektedir. Kali Linux makinesinin sahip olduğu IP ve subnet adreslerine Şekil 2.23.'de görüldüğü gibi "ifconfig" komutu ile erişmek mümkündür.

Şekil 2. 24. Kali Linux ifconfig komutu sonucu

Şekil 2.24.'de elde edilen Nmap tarama sonucu ile ilgili subnet üzerinde olan cihazlar tespit edilmiştir. 1, 2 ve 254 ile biten makine ip'leri Vmware'de var olan sistem ile IP Bridge yapıldığından kendi IP adresi ile birlikte bağlı tüm cihazlar tespit edilmiştir.



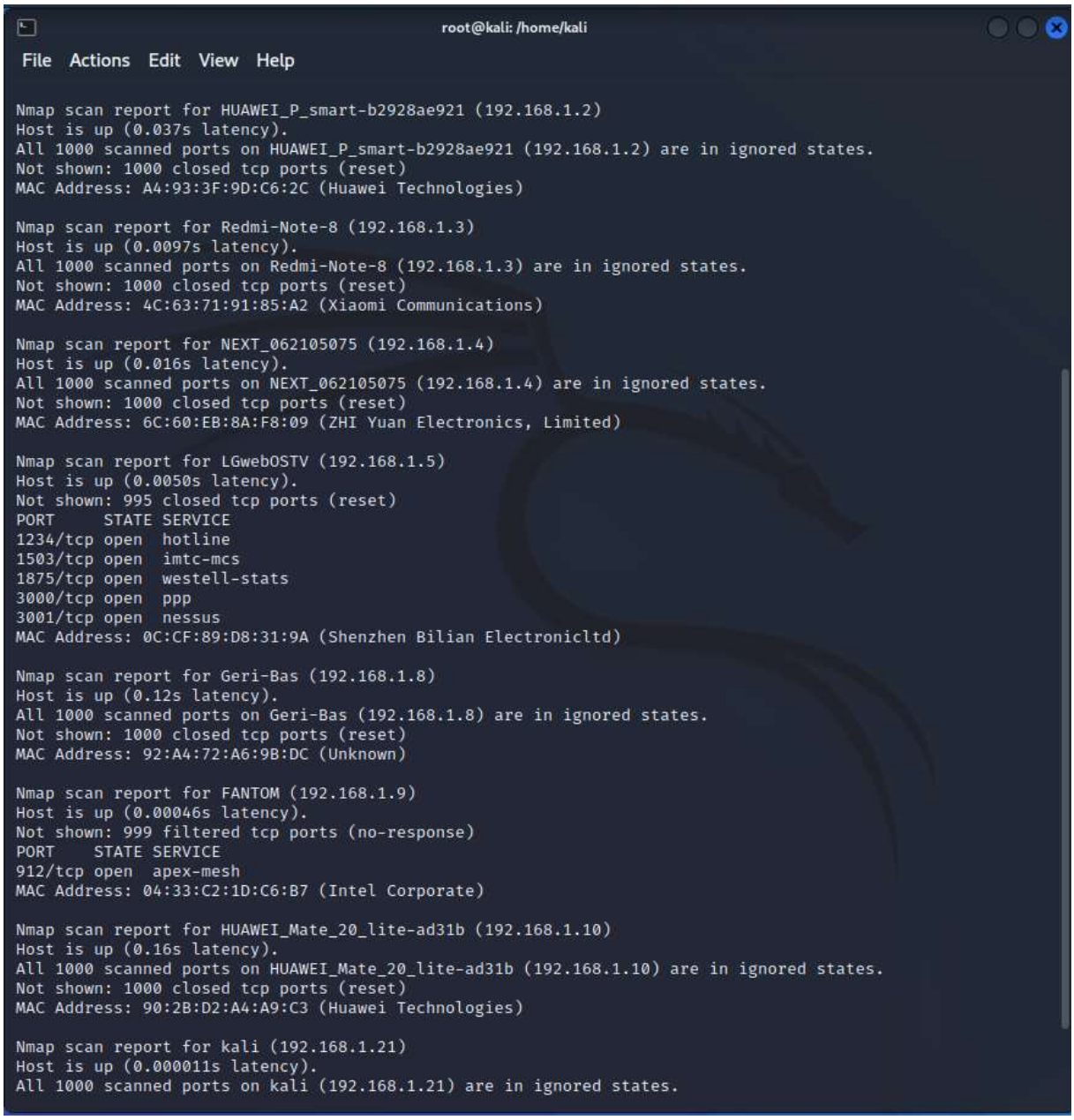
Şekil 2. 25. Tespit edilen cihazlar

Şekil 2.25.'te 1, 2, 3, 4, 5, 6, 8, 10 ve 21 ile biten IP adresine ait 9 adet cihaz saptanmıştır. 21 ile biten ip adresi Kali Linux cihazının kendisi, 1 nolu IP adresi modem, 2 nolu Huawei_P_Smart, 3 nolu IP adresi Redmi_Note_8, 4 Nolu IP adresi NEXT_062105075, 5 nolu IP adresi LGWebOSTV, 6 nolu IP adresi U14482KF, 8 nolu IP adresi Geri-Bas, 10 nolu IP adresi HUAWEI_Mate_20_lite-ad31b cihazları bulunmuştur.

2.2.2. TCP Servislerinin Saptanması

Güvenlik açıklarının sömürülmesi işleminde hedef makinenin tcp servislerinin saptanması oldukça kritik bir noktadır. Bu bölümde nmap yazılımı kullanılarak hedef sistem üzerindeki tcp bazlı servisler tespit edilmiştir. Bu işlem için nmap –sS parametresi kullanılarak

hedef makine üzerine syn paketleri gönderilmiştir. Bunun sonucunda hangi servis ve portların açık olduğu bilgisi döndürülmüştür.



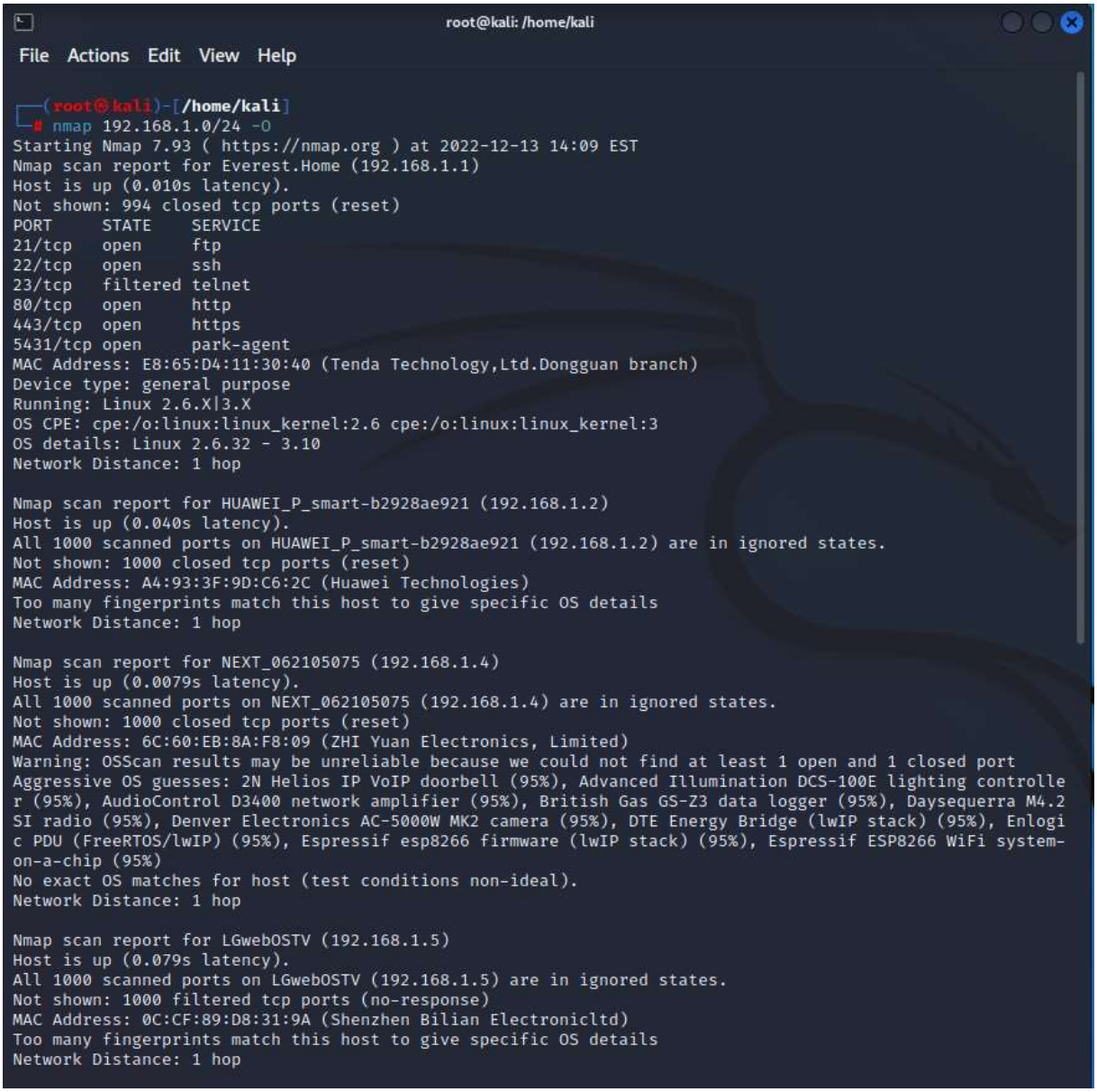
Şekil 2. 26. Açık TCP Portları

Şekil 2.26.'te 1234, 1503, 1875, 3000, 3001 ve 915 tcp portlarının açık olduğu bilgisine ulaşılmıştır. Hedef makine olarak seçilen diğer cihaz IP adresleri kullanılarak ilgili cihazların tcp servis bilgilerine aynı yöntem ile ulaşmak mümkündür.

2.2.3. İşletim sisteminin Saptanması

Bu bölümde nmap aracı ile tespit edilen ip adreslerinin işletim sistemi bilgileri gene nmap aracı ile tespit edilmiştir. Bunun için nmap –O parametresi kullanılmıştır. Bu parametre

her zaman doğru sonuç döndürmese de çoğunlukla doğru sonuç döndürmektedir. Şekil 2.27. ve Şekil 2.28.'de sırasıyla cihazların işletim sistemi bilgileri seçenekleri gösterilmiştir.

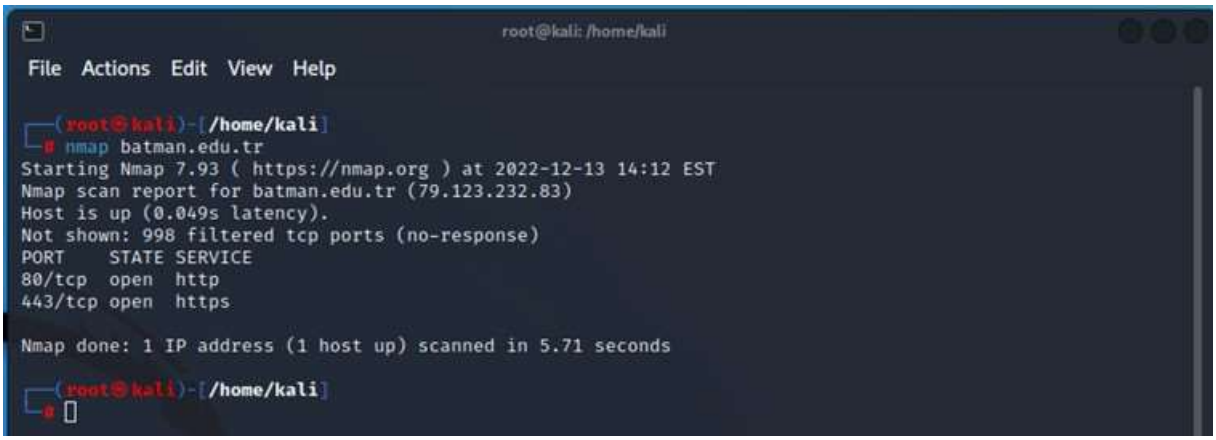


Şekil 2. 27. Cihazlara ait işletim sistemi ve diğer bilgiler

Şekil 2. 28. Cihazlara ait işletim sistemi ve diğer bilgiler 2

2.2.4. Web Sitesi DNS İsimlerini Tarama

Bu bölümde Nmap aracı ile DNS'ler ile ilgili tarama yapılıp, domaine ait port tarama bilgileri elde edilmiştir. Şekil 2.29.



Şekil 2. 29. DNS tarama örneği

3. AĞ SALDIRI YÖNTEMLERİ

3.1. Tanımlar

3.1.1. 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. (VMware, “2019 Gartner Magic Quadrant'da Lider Oldu”, 2022)

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

3.1.2. İşletim Sistemleri

Bu çalışmada yer alan uygulamaların üzerinde çalışacağı işletim sistemlerinden bahsedilmiştir.

3.1.2.1.FREEBSD İşletim Sistemi

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. (FreeBSD, FreeBSD Hakkında,2022)

3.1.2.2.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. (Kali Linux, What is Kali Linux,2022)

3.1.2.3.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. (Microsoft Windows, Vikipedia Sözlük Microsoft Windows,2022)

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. (En Son Haber, Dünyada en çok kullanılan masaüstü işletim sistemi belli oldu, 2022)

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. (Microsoft Windows, Microsoft Release Information, 2022)

3.1.2.4.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. (Pfsense, Getting-Started, 2022)

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.

3.1.2.5.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. (Snort, Snort Community, 2022)

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

3.2. Saldırı Tespit Sistemleri

3.2.1. 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. (Çavuş, M.F. ve Kurt, H.S.(2017))

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. (Şen, Şenol ve Yerlikaya Tarık, Akademik Bilişim 2013)

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.

3.2.2. 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).

3.2.3. 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. (Saldırı Tespit Sistemleri, İTÜ Bilgi İşlem Dairesi Başkanlığı, 2022)

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

3.2.4. 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. (Çavuş, M.F. ve Kurt, H.S. (2017) Kamu alanında yapılan bu çalışmada açık kaynak kodlu yazılımların güvenli olması, toplam tedarik etme maliyetleri ve diğer etkenler ile bir adım önde olduğu belirtilmektedir.

3.2.5. Örnek Ağ Topolojisi

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	16 GB DDR4

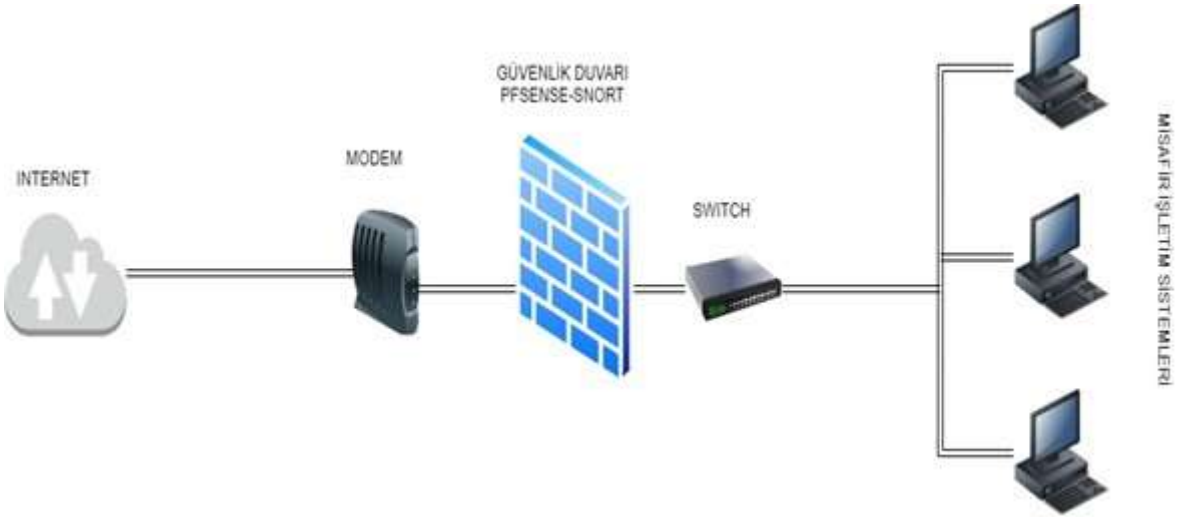
Tablo 1.1. Donanım Özellikleri

Sunucu İşletim Sistemi	Windows 10 Enterprise
Güvenlik Duvarı İşletim Sistemi	FreeBSD Pfsense 2.4.5, Snort 2.4.5

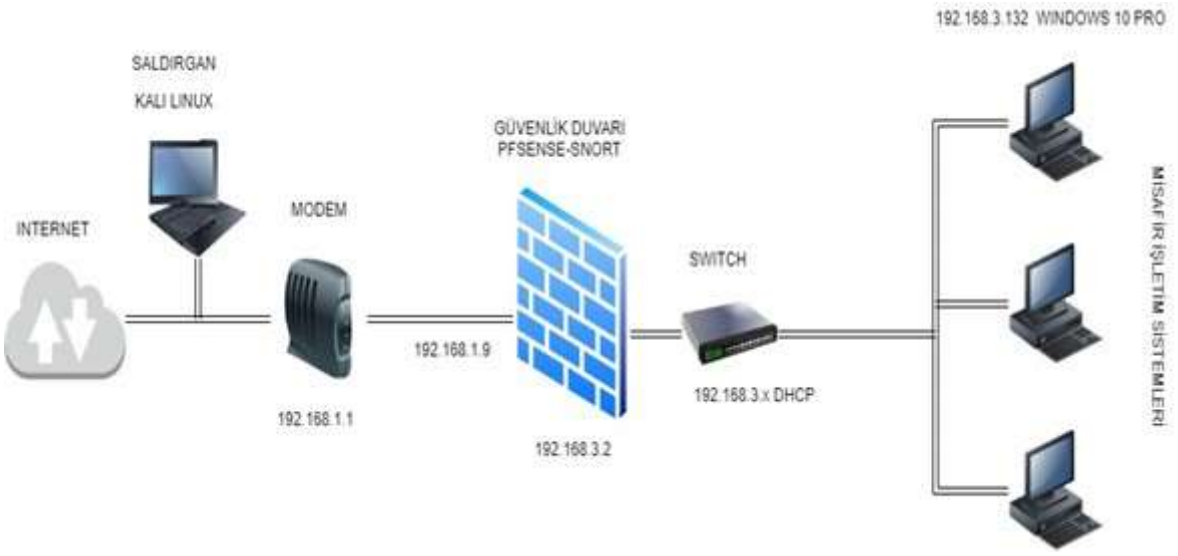
Misafir İşletim Sistemi	Windows 10 Pro
Saldırgan İşletim Sistemi	Kali Linux 2022

Tablo 1.2. Kullanılan Yazılım ve Sürüm Numaraları

Projede uygulanacak olan temel topoloji şeması Şekil 3.1 de belirtilmiştir. Çalışma içerisin de kullanılacak olan topoloji içerisinde yer alan sistemlere ait ip adres bilgisi ve rolleri Şekil 3.2'de gösterilen topolojideki gibi olmaktadır.



Şekil 3. 1. Temel Topoloji Şeması Genel Konumlar

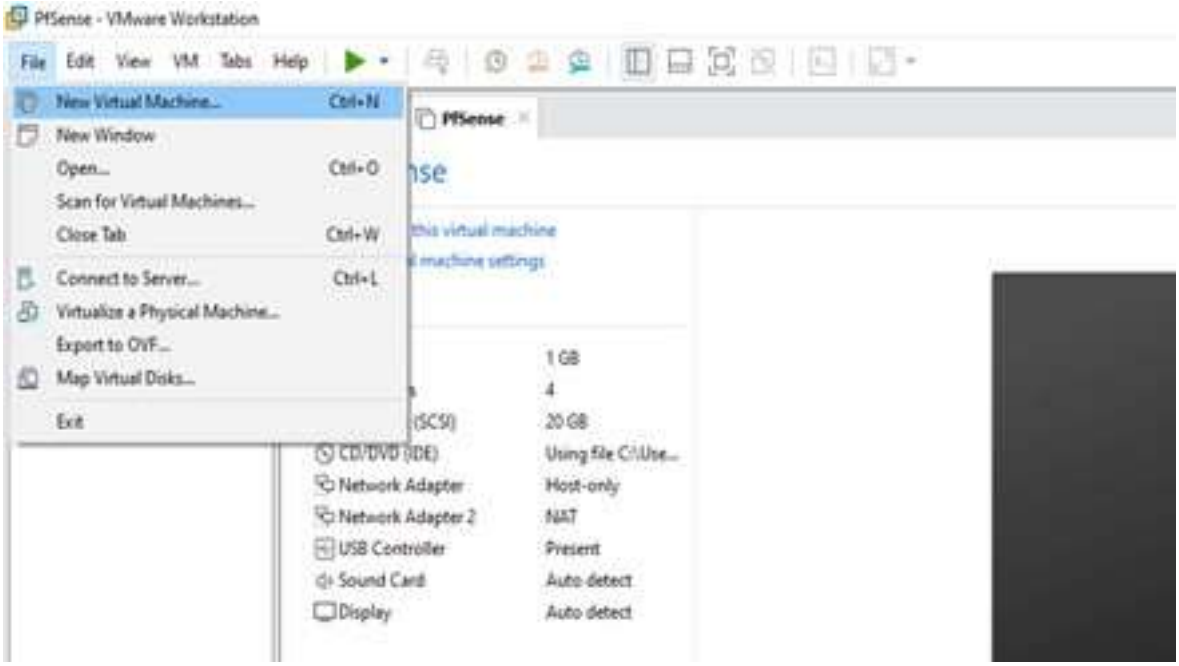


Şekil 3. 2. Genel Ağ Topolojisi Saldırgan Konumu

3.3. Kurulumların Yapılması ve Örnek Ağ Oluşturulması

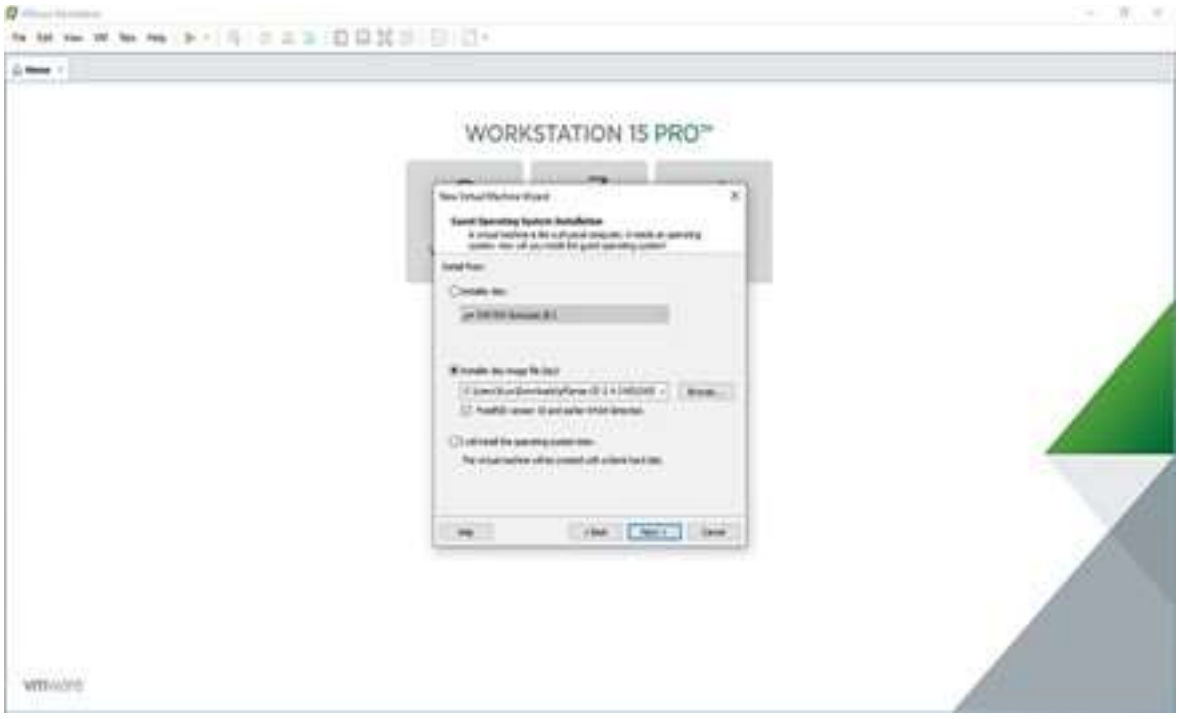
3.3.1. Vmvare Kurulumu

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.

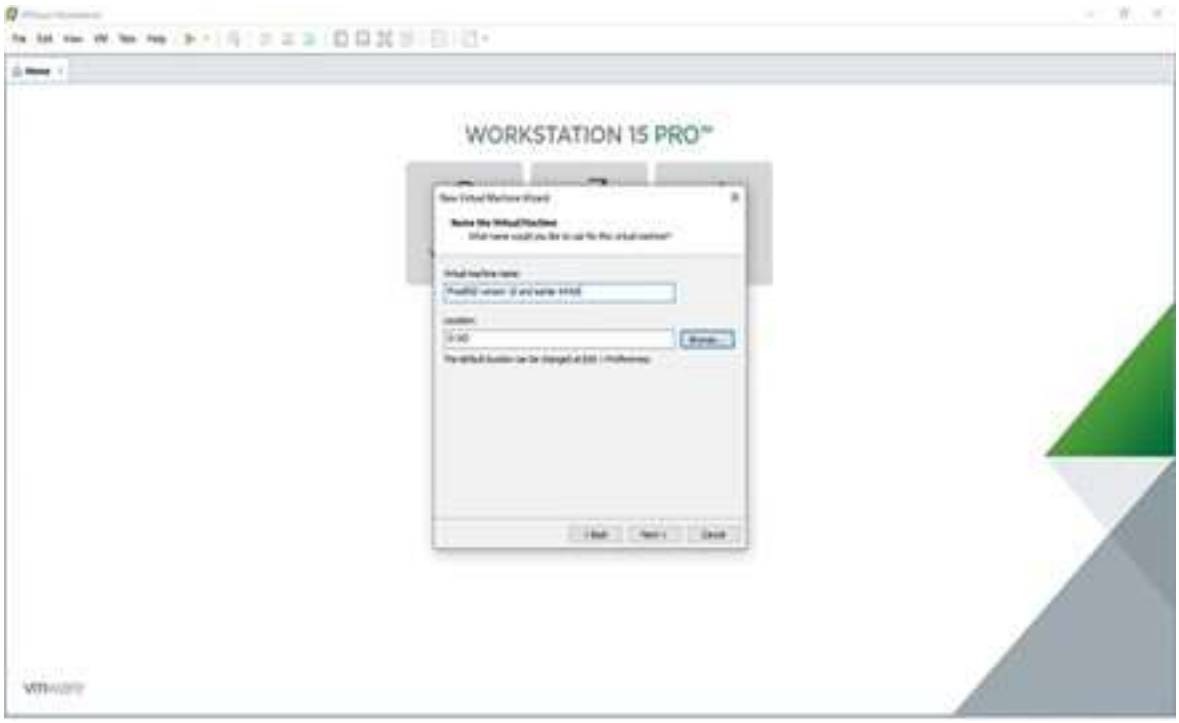


Şekil 3. 3. Yeni Sanal Makina Oluşturulması

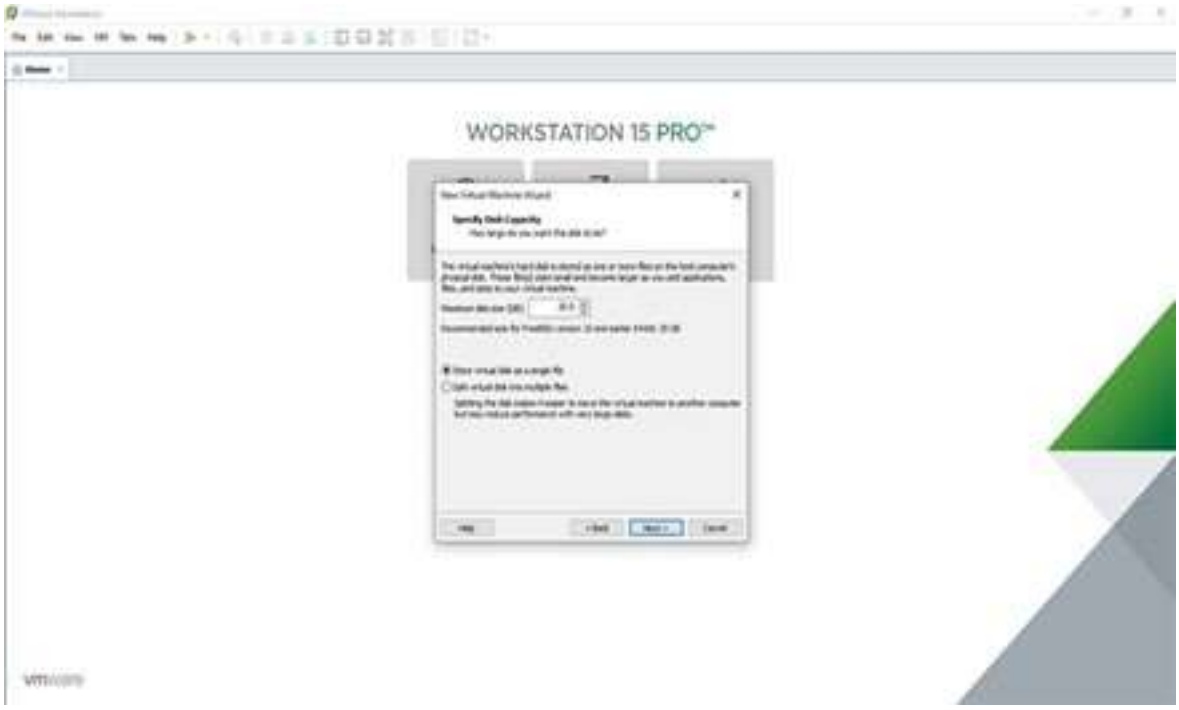
Şekil 3. 4. Tipik Seçim



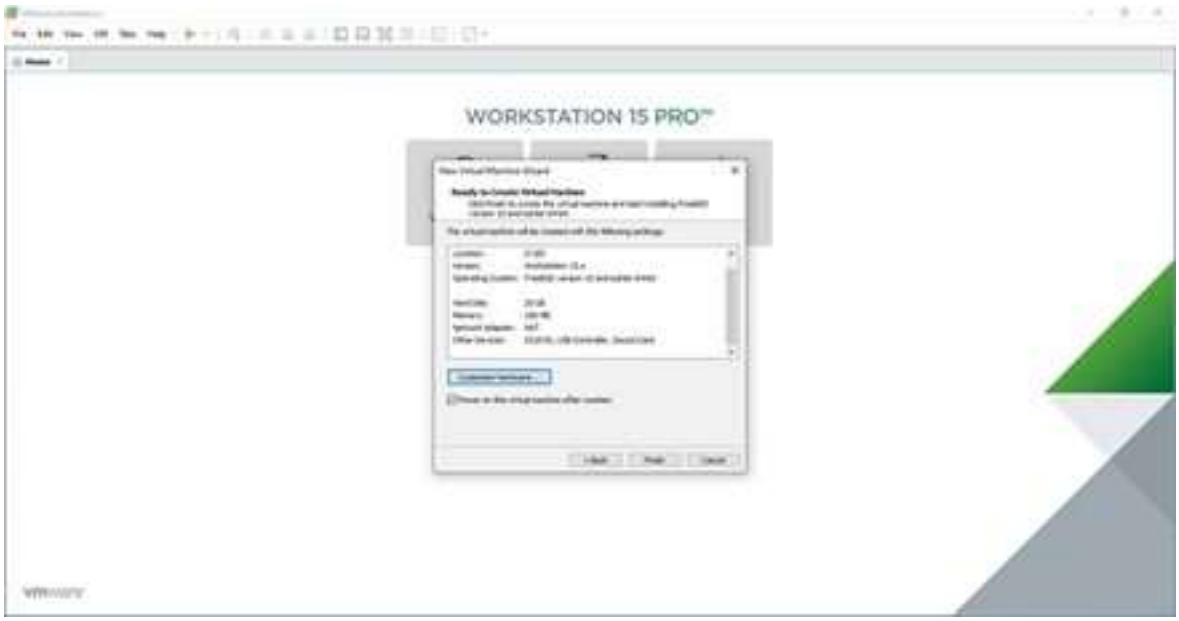
Şekil 3. 5. Kurulacak Sistemin ISO kurulum dosyası seçimi



Şekil 3. 6. Kurulacak olan işletim sisteminin konumu ve sanal dosya adının belirlenmesi



Şekil 3. 7.Kurulacak sistemin sanal üzerinde kapasitesinin belirlenmesi



Şekil 3. 8. Sanal Sistem Konfigürasyonu Listesi

3.3.2. PfSense Kurulumu

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

Şekil 3. 9. Pfsense ISO dosyası indirme

Sanal makine için aşağıda belirtilen kaynaklardan yararlanılarak sanal makina oluşturulmuştur. Tablo 1.3.

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

Tablo 1.3. Pfsense için Sanal Makine Özellikleri

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

Şekil 3. 10. Pfsense Telif Hakları

Sanal makinede Pfsense güvenlik duvarını başlattığımız anda ilk karşımıza çıkan ekran telif hakları ve dağıtım bildirimidir Şekil 3.10. Kabul edilerek devam edilir. Şekil 3.11.

Şekil 3. 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 3. 12. Keymap seçenekleri

Kullanacağımız klavye tipi seçildikten sonra devam edilir. Şekil 3.12.

Şekil 3. 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

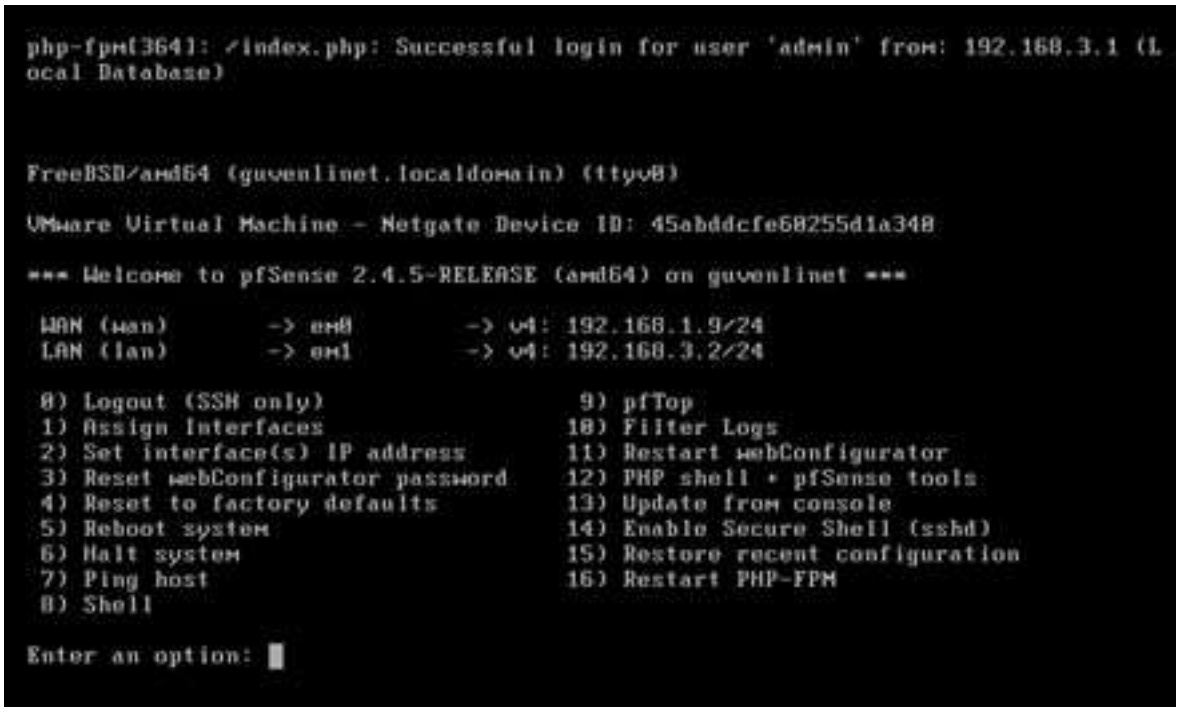
4. son seçenekte yine otomatik olarak ZFS dosya sisteminde kurulumu başlatabilirsiniz. Şekil 3.13.

Şekil 3. 14. Pfsense Kurulum

Bu adımda ise gerekli dosyalar ayarlanıp kuruluma devam etmektedir. Şekil 3.14.

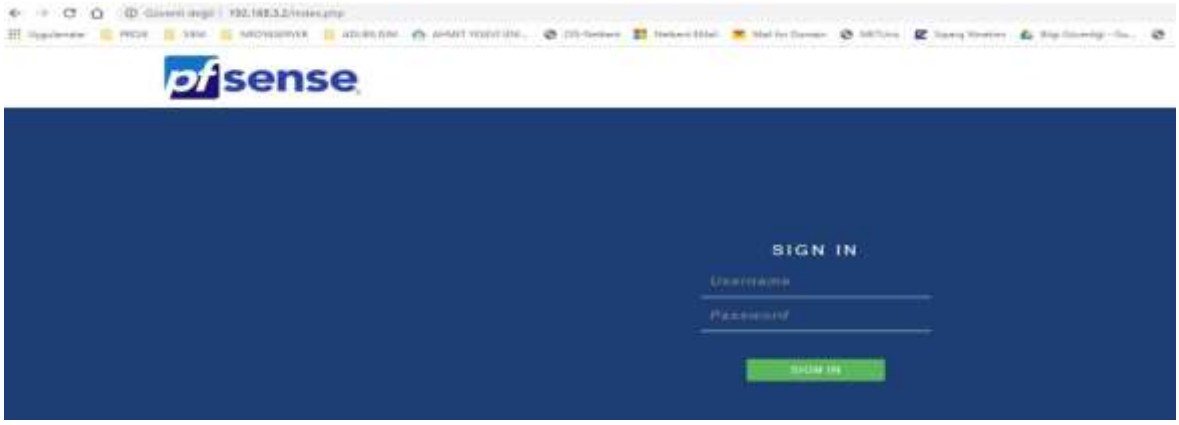
Şekil 3. 15. Manuel Yapılandırma Sorgulama Ekranı

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 3. 16. Pfsense Başlangıç ve Yapılandırma Seçenekleri

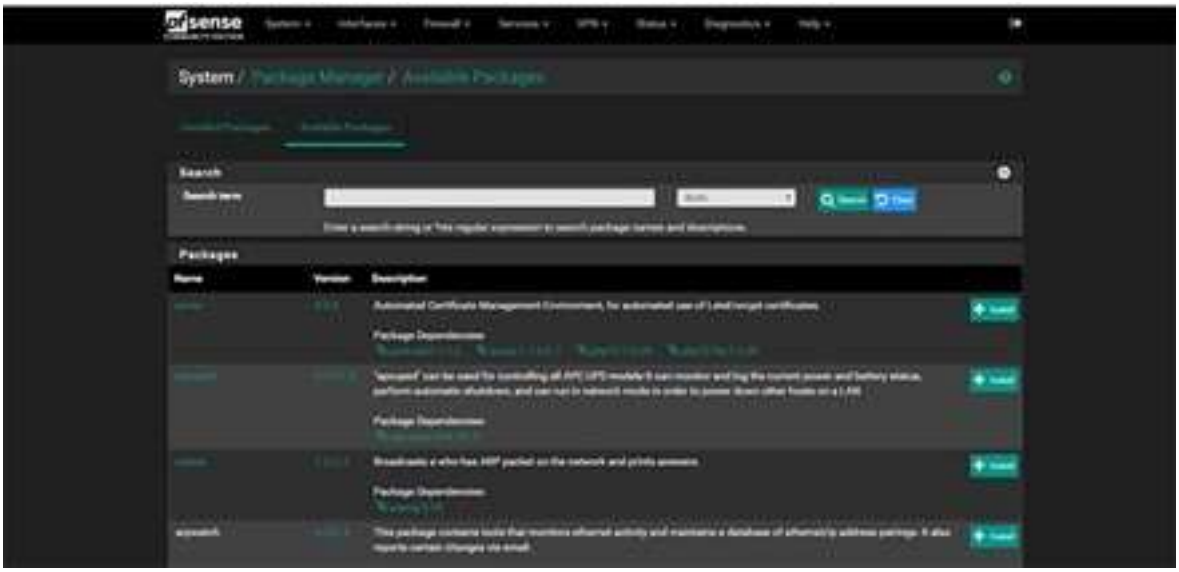
Makinemizi açtığımızda karşımıza yapılandırma ekranında LAN ve WAN IP adreslerini değiştirmek için 2.seçenek olan “Set interface IP adress” seçeneğini seçerek değiştirebiliriz. LAN ve WAN IP adresleri default olarak otomatik verilmektedir. Söz konusu yapılandırma Şekil 16. daki gibi yapılmıştır. Yapılandırma 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 3.17.



Şekil 3. 17. Pfsense Erişim Ekranı

3.3.3. Snort Kurulumu

Pfsense kurulumu yapıldıktan sonra Pfsense web arayüzünden Snort paketini kurulumu yapılır. Bunun için “System / Package Manager / Available Package” kısmına geçilir. Şekil 3.18.



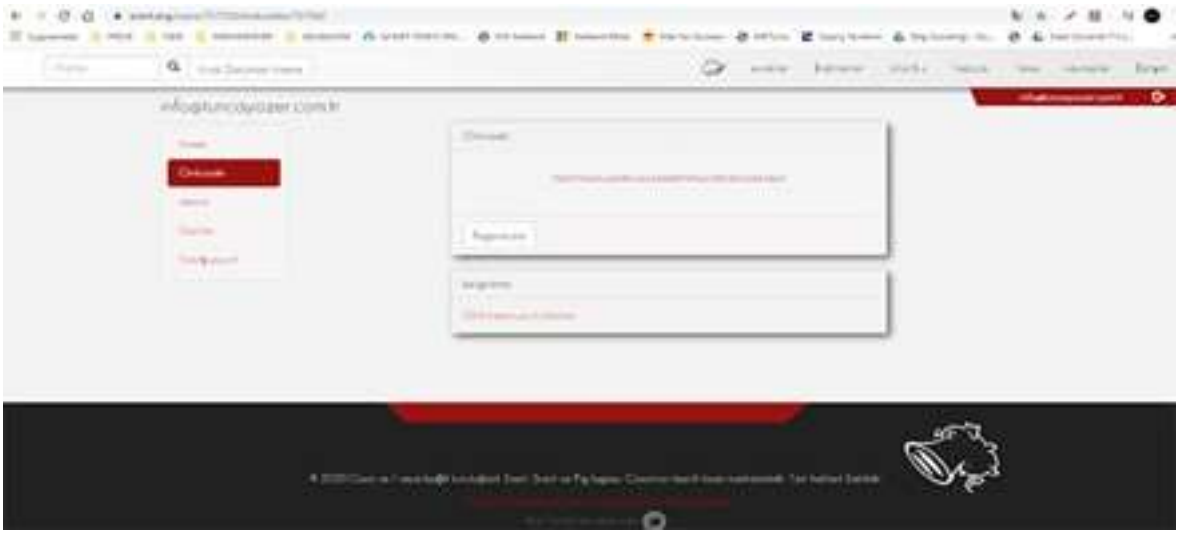
Şekil 3. 18. Pfsense mevcut paketler bölümü

Paket kurulumunu sırasıyla “Available Package” bölümünden gelen listede Snort’u bulunur ve install (kur) ile paket çevrimiçi olarak indirilip kurulum gerçekleşir. Şekil 3.19. ve Şekil 3.20.

Şekil 3. 19. Paketler Listesi

Şekil 3. 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 3.21.



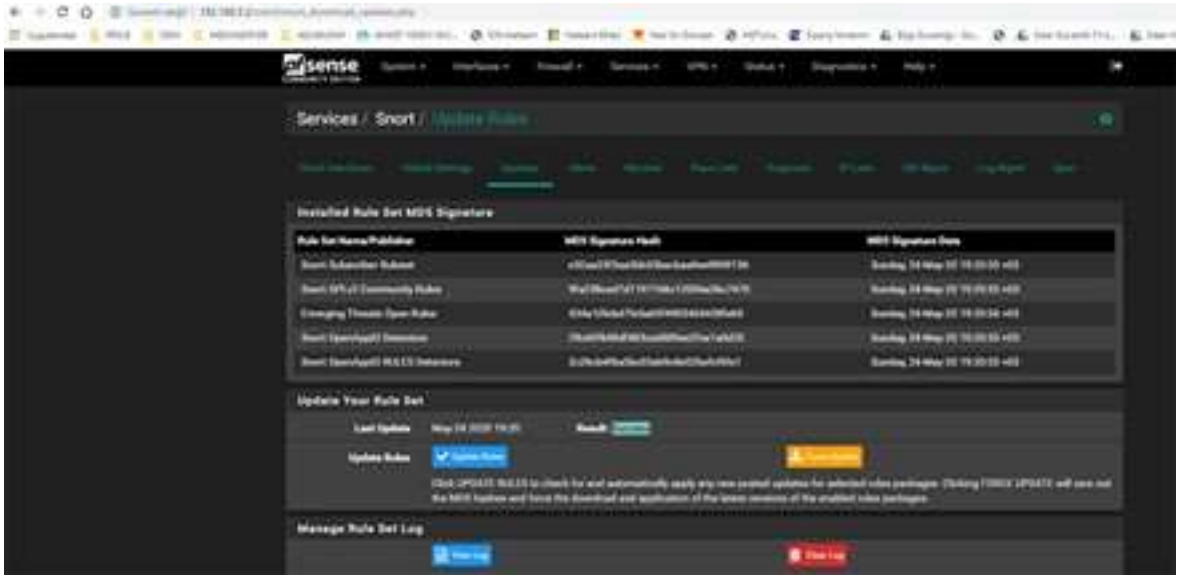
Şekil 3. 21. Snort OinkCode ekranı

Pfsense web ara yüzünde Genel Ayarlar (Global Settings) sekmesine gelinir, **install snort VRT Rules** kutucuğunu işaretlenir ve siteden alınan oinkcode kodu Şekil 3.22. de görüldüğü üzere yazıp alt kısımda Save (kayıt) işlemi yapılır.

Şekil 3. 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 3.23 ve Şekil 3.24.

Şekil 3. 23. Snort Rule Update İşlemi



Şekil 3. 24. Snort Rule Update İşleminin Bitimi

3.3.4. Kurban Sistemlerin Kurulumu

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;

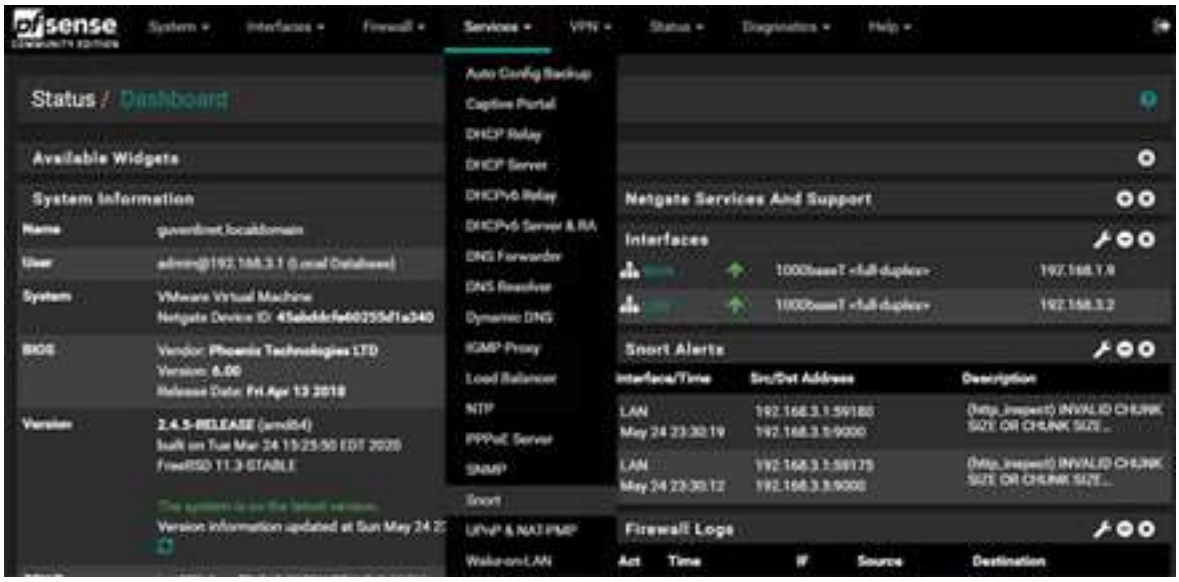
İşlemci	2 Core
Bellek	1 GB
Kapasite	20 GB
Network	1 adet network adaptörü

Tablo 1.4. Kali Linux ve Windows 10 Pro Sanal Makine Özellikleri

3.4. Sistem Entegrasyonu ve Test

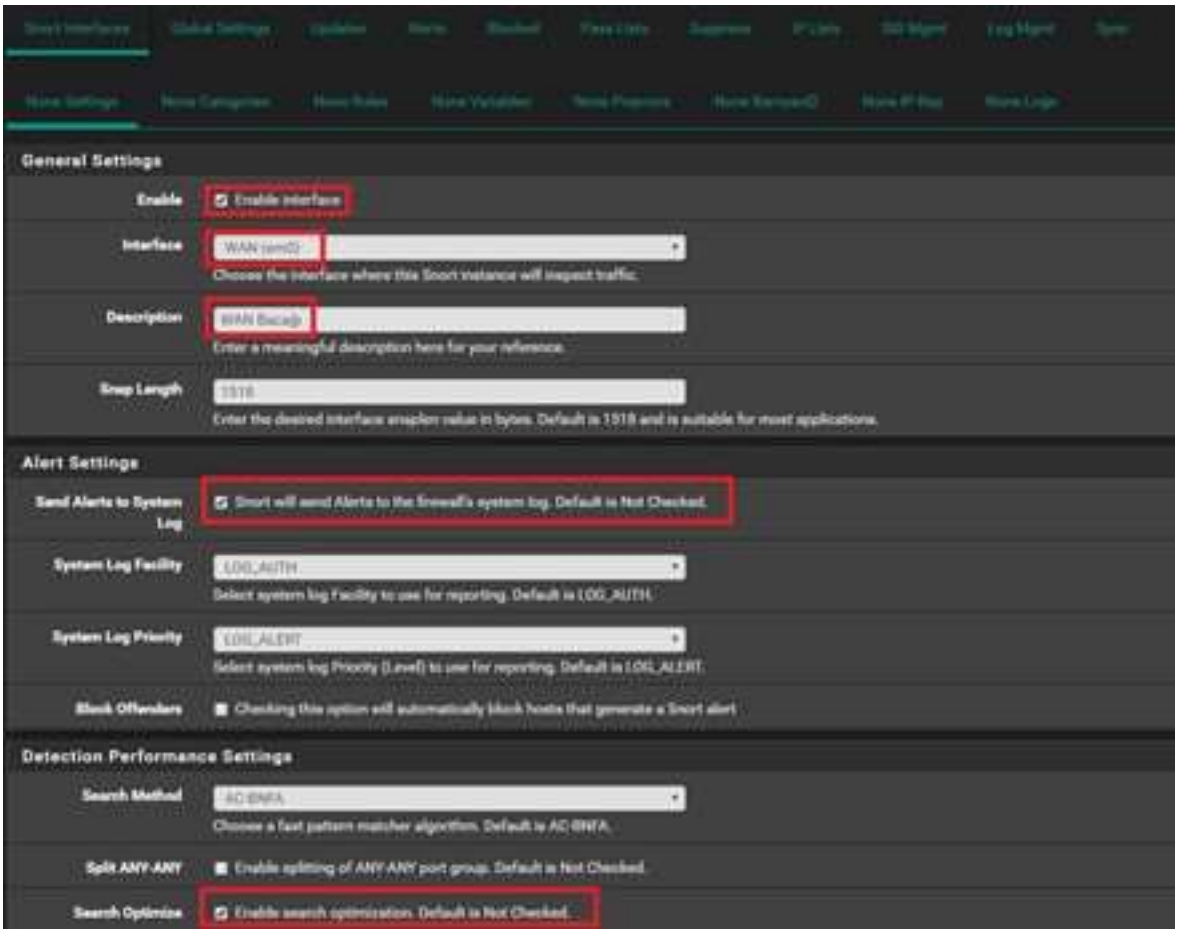
3.4.1. Snort Aktif Etme

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 3.25.

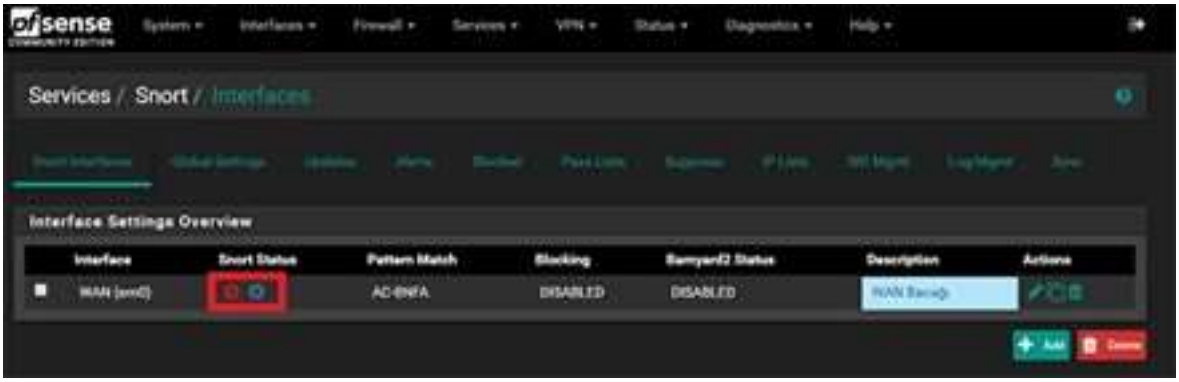


Şekil 3. 25. Snort Servisi Seçimi

Gelen ekranda Snort Interfaces kısmında Add yaparak network bacaklarının ayarlamaları yapılacaktır. Öncelikli olarak Wan Network Bacağı daha sonrasında Lan Network Bacağının ayarlamaları yapılır. Şekil 3.26. ve Şekil 3.27.

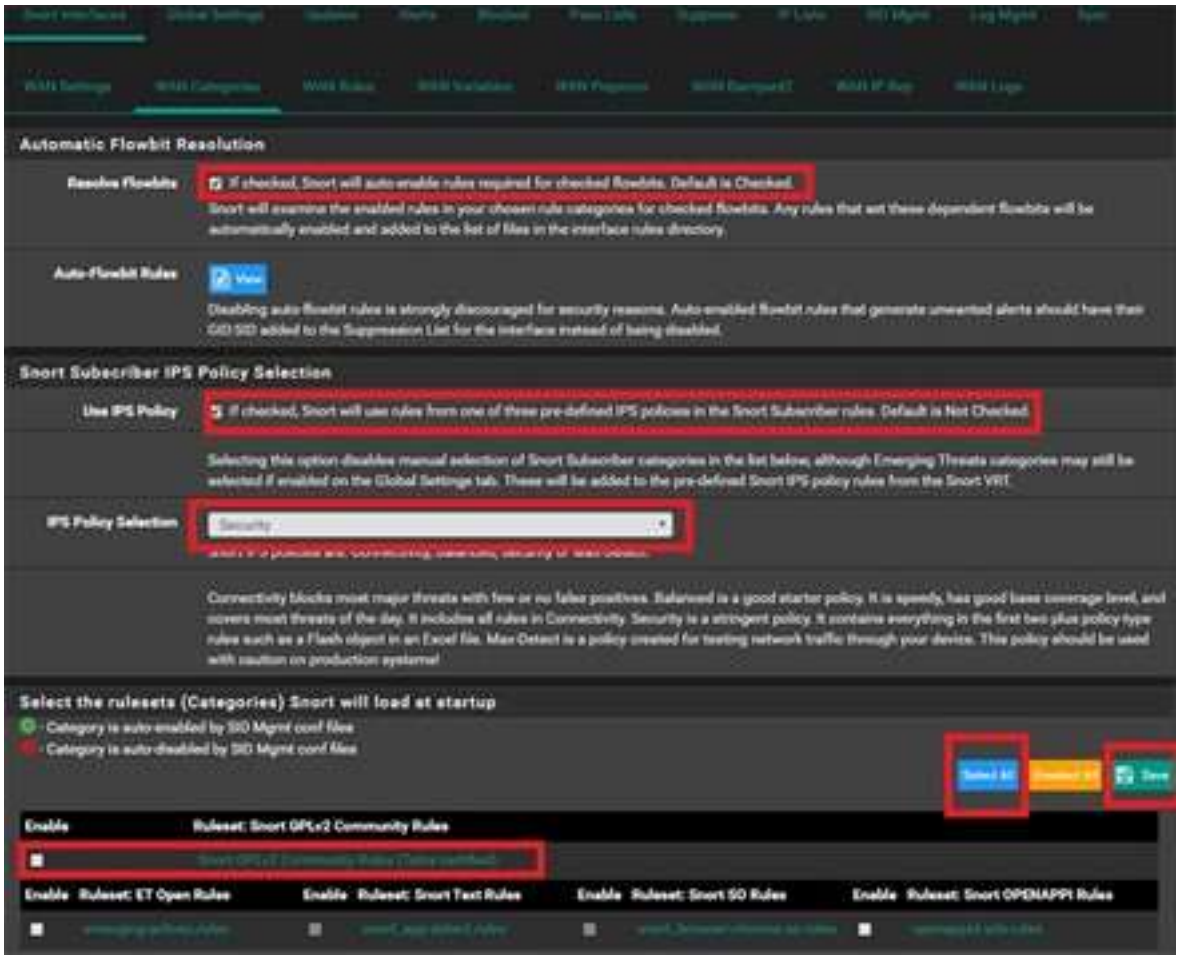


Şekil 3. 26. Wan Network Bacağını Ayarlama



Şekil 3. 27. Wan Bacağı

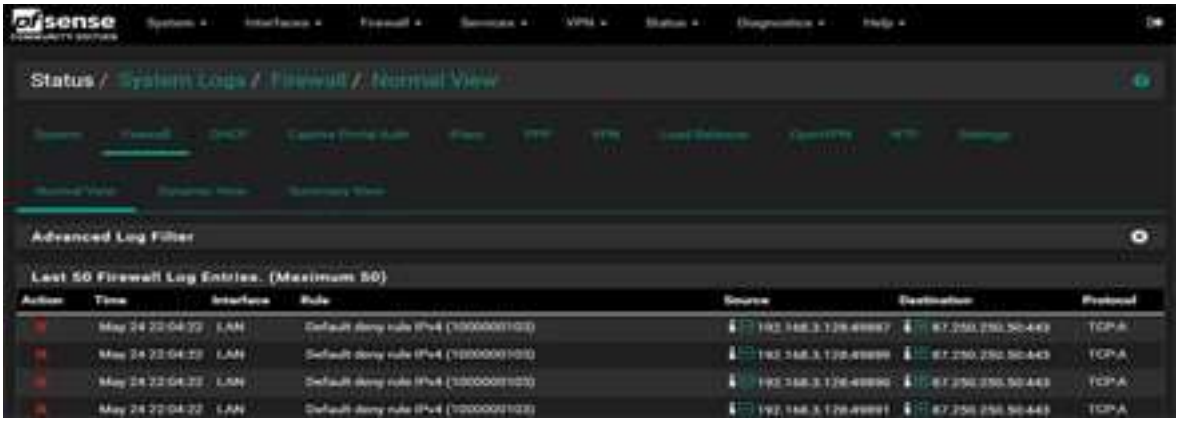
Network ağının hangi kurallarla korunacağı hususunda seçenekler seçimi yapılır. Community sürümünü yüklediğimizden, community kuralları aktif olacaktır. Şekil 3.28.



Şekil 3. 28. 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 3.29.



Şekil 3. 29. Firewall Log Görüntüsü

3.5. Model Sisteme Saldırı Yöntemleri

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.

3.5.1. Keşif Saldırıları

3.5.1.1. NMAP

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 ……

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*

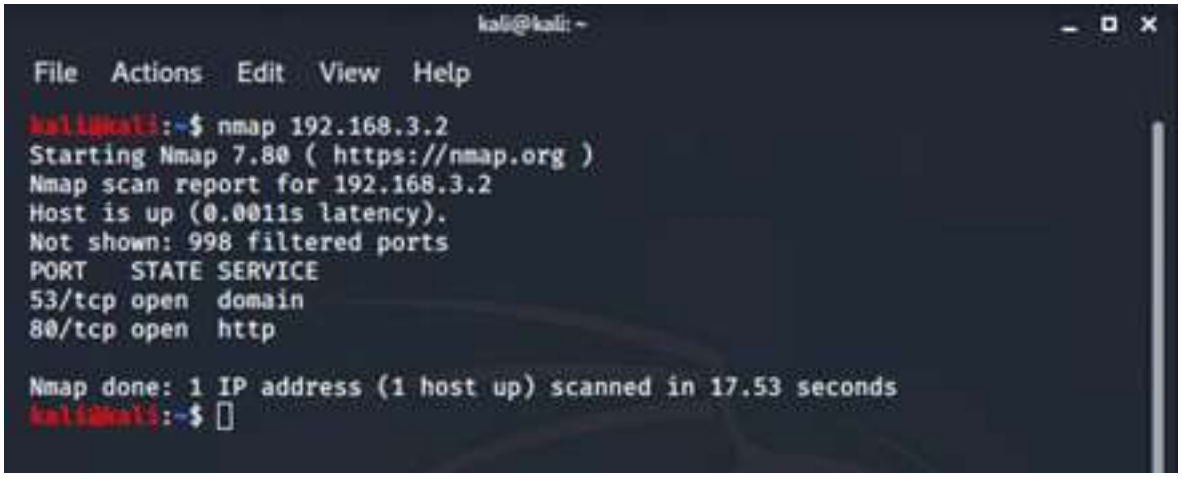
Host is up (0.010s latency).

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. 30. PfSense Makinasına Nmap Keşfi

Şekil 3. 31. Snort Nmap UDP paketlerinin tespiti

3.5.2. Atak Örnekleri

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. (Kaspersky, DDoS Atağı Nedir, 2022)

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. (ISSA Turkey, DoS, DDoS Atakları, 2022)

- 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

3.5.2.1. 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. (Penetration Testing, Penetration Testing Scanning, 2022). Şekil 3.32. Attack sonucu Şekil 3.33. ‘te gösterilmiştir.

Şekil 3. 32. 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. 33. Snort Arayüzü Push Attack

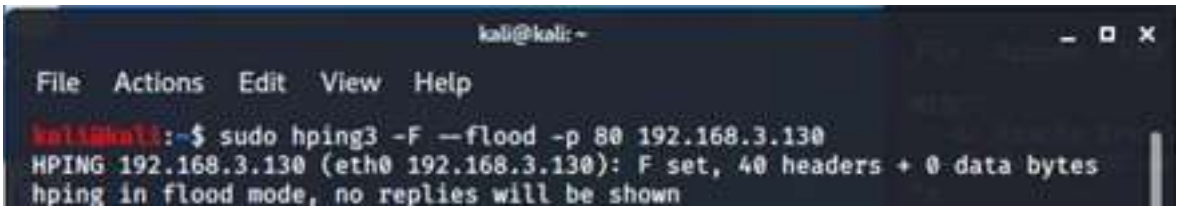
3.5.2.2. UDP Atak

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. (Penetration Testing, Penetration Testing Scanning, 2022)

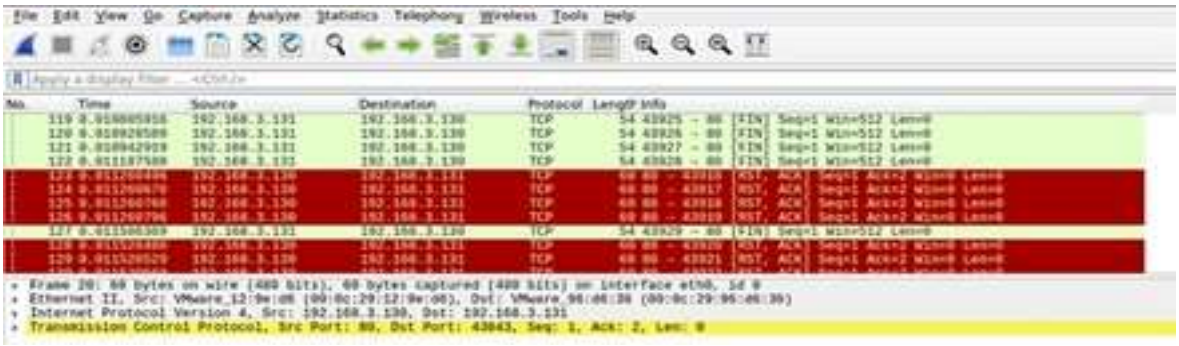
Saldırı topolojimizde yer alan Kali Linux İşletim sisteminden Windows 10 Pro işletim sisteminde IIS (Internet Information Service) kurulu sisteme yapılacaktır. Güvenlik duvarımıza "*alert udp any any -> 192.168.3.132 any (msg: "UDP Flood Dos"; sid:1000001;)*" rolünü custom.rules kısmına ekliyoruz. Burada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

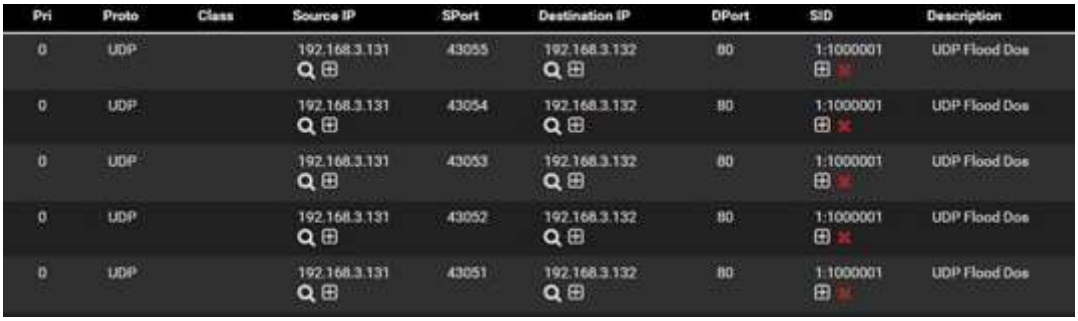


Şekil 3. 34. Hping3 paket gönderme



Şekil 3. 35. 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. Etkin bir saldırı için birden çok PC ile saldırı yapılması gerekmekle birlikte networkün band genişliğine göre değişmektedir.



Şekil 3. 36. Snort UDP Atak Yakalama Görüntüsü

Şekil 3. 37. Internet Information Services web arayüzü

3.5.2.3. 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. Penetration Testing, Penetration Testing Scanning, 2022)

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 3.38.

Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
0	TCP		192.168.3.131	39794	192.168.3.132	80	1:1000001	Reset Dos
0	TCP		192.168.3.131	39793	192.168.3.132	80	1:1000001	Reset Dos
0	TCP		192.168.3.131	39792	192.168.3.132	80	1:1000001	Reset Dos
0	TCP		192.168.3.131	39791	192.168.3.132	80	1:1000001	Reset Dos

Şekil 3. 38. Reset Dos Atak

3.5.2.4. 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. (Penetration Testing, Penetration Testing Scanning, 2022)

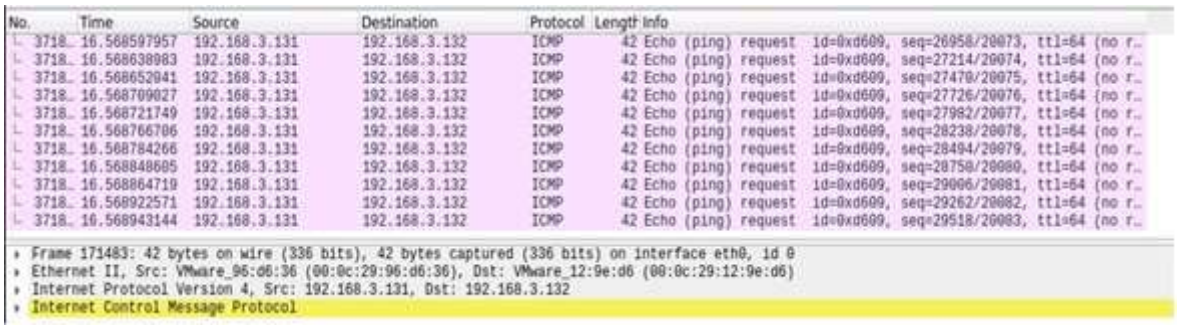
Güvenlik duvarına (Snort) saldırganın yapacağı bu atağa karşı alarm rolümüzü tanıtıyoruz.

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

Saldırgan aşağıdaki komutu icra etmektedir.

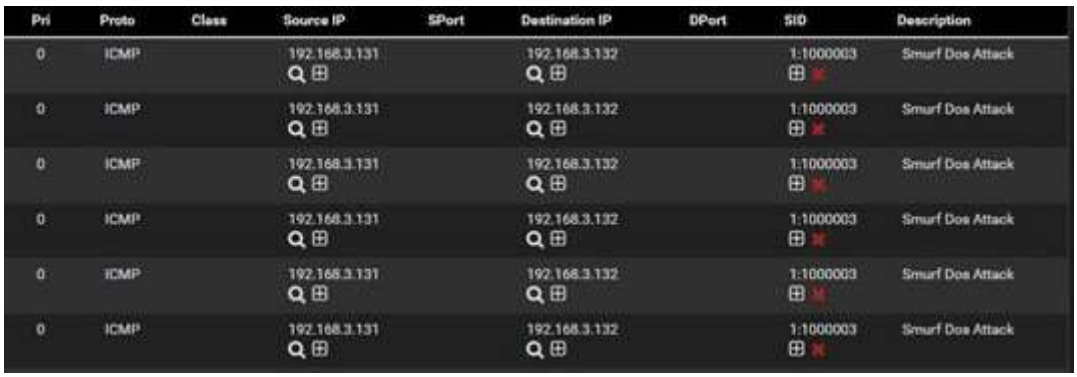
"hping3 --icmp --flood -c 1000 --spoof 192.168.3.131 192.168.3.132"

Gönderilen paketler Wireshark aracı ile gözlemlenmiştir. Şekil 3.39.



Şekil 3. 39. Wireshark ICMP atakları

Snort saldırılar karşısında alarm üretmektedir. Şekil 3.40.



Şekil 3. 40. Snort ICMP atakları

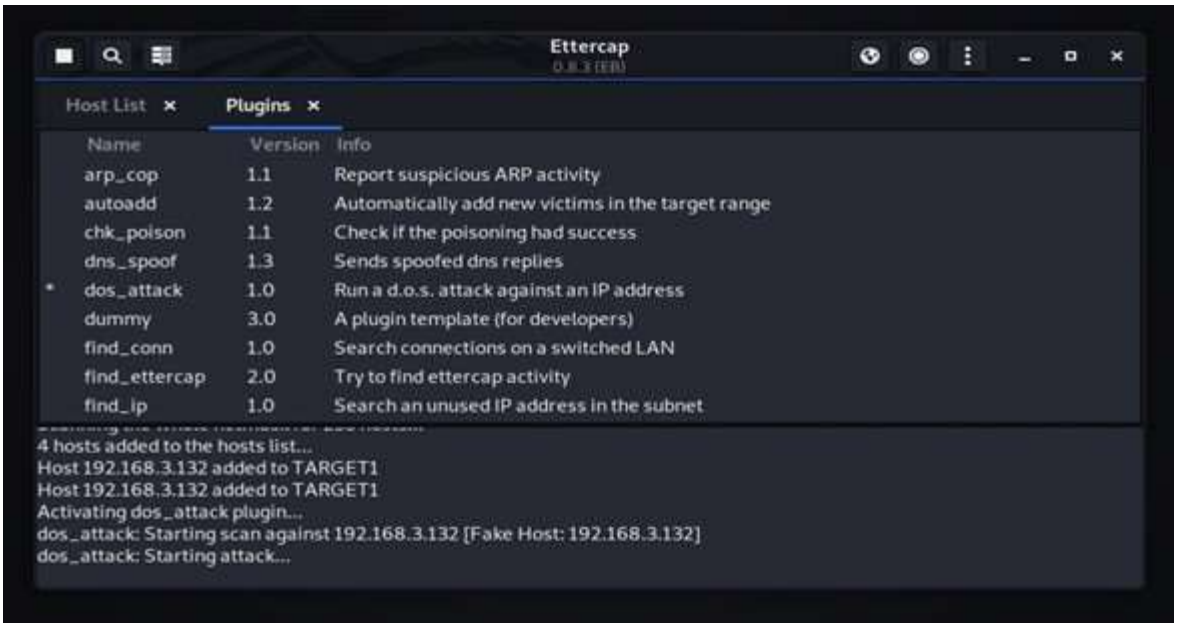
3.5.2.5. TCP Syn Atak

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. Penetration Testing, Penetration Testing Scanning, 2022)

Güvenlik Duvarına (Snort) atak alarm rolünü eklenir.

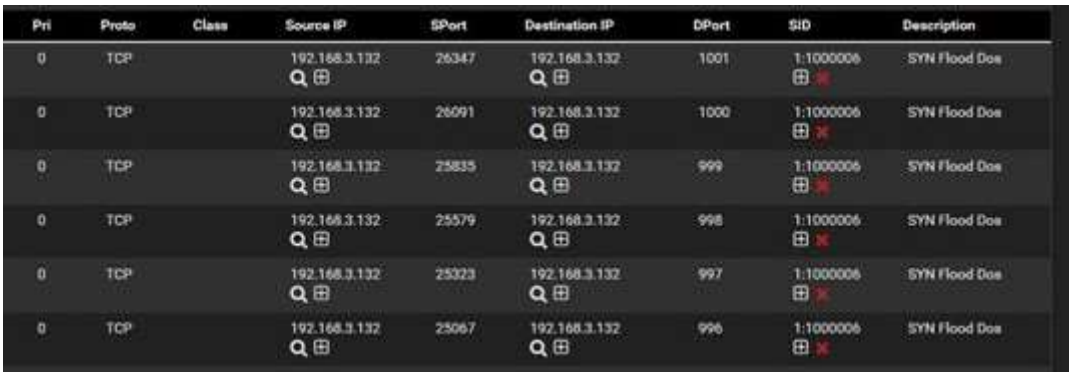
"*alert tcp any any -> 192.168.3.132 any (msg:"SYN Flood Dos"; flags:S; sid:1000006;)"*

Saldırgan atak yapmak için ettercap uygulamasını kullanmaktadır. Ayrıca atağı fake dediğimiz yalancı IP adresi ile karşı tarafın IP adresi ile yapmaktadır. Şekil 3.41.



Şekil 3. 41. Ettercap dos_attack

Saldırı sonucunda daha önce tanımlanan alarm rolünü snort tanımlayarak alarmı vermektedir. Şekil 3.42.



Şekil 3. 42. Snort Ettercap Dos Atağı alarmı

3.5.2.6. 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. (Penetration Testing, Penetration Testing Scanning, 2022)

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 3.43.

```
:~$ sudo git clone https://github.com/gkbrk/slowloris.git
Cloning into 'slowloris'...
remote: Enumerating objects: 5, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 103 (delta 1), reused 2 (delta 1), pack-reused 98
Receiving objects: 100% (103/103), 18.17 KiB | 6.06 MiB/s, done.
Resolving deltas: 100% (48/48), done.
```

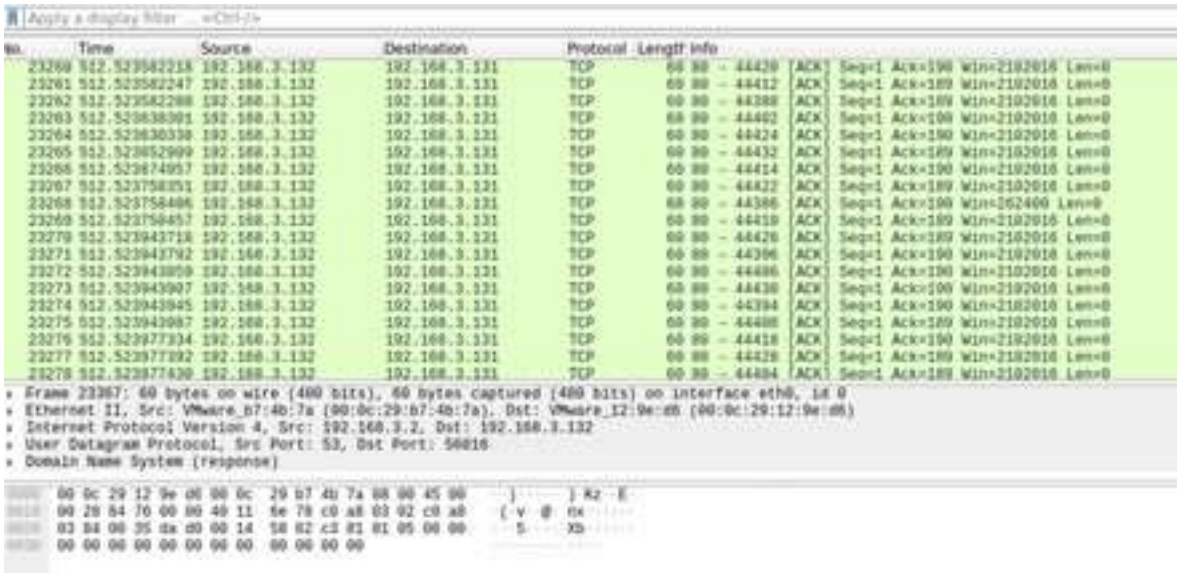
Şekil 3. 43. Slowloris uygulamasını indirme

Slowloris uygulaması atak için kullanılır. Şekil 3.44.

```
python3 slowloris.py 192.168.3.132
Attacking 192.168.3.132 with 150 sockets.
Creating sockets...
Sending keep-alive headers... Socket count: 0
Sending keep-alive headers... Socket count: 0
Sending keep-alive headers... Socket count: 0
Sending keep-alive headers... Socket count: 150
Sending keep-alive headers... Socket count: 150
Sending keep-alive headers... Socket count: 150
Sending keep-alive headers... Socket count: 150
Sending keep-alive headers... Socket count: 150
Sending keep-alive headers... Socket count: 150
Sending keep-alive headers... Socket count: 150
Sending keep-alive headers... Socket count: 150
Sending keep-alive headers... Socket count: 150
```

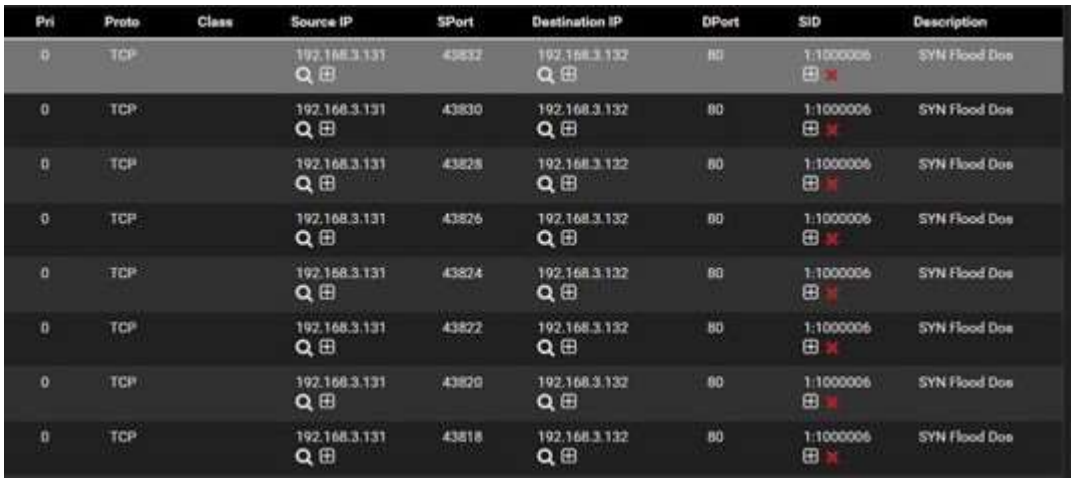
Şekil 3. 44. Slowloris Atak

Wireshark ile gönderilen paketler izlenir. Şekil 3.45.



Şekil 3. 45. Wireshark Slowloris paketleri

Snort güvenlik duvarın daha önceden tanımlanan SYN Flood rolü alarm vermektedir. Şekil 3.46.



Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
0	TCP		192.168.3.131	43832	192.168.3.132	80	1:1000006	SYN Flood Dos
0	TCP		192.168.3.131	43830	192.168.3.132	80	1:1000006	SYN Flood Dos
0	TCP		192.168.3.131	43828	192.168.3.132	80	1:1000006	SYN Flood Dos
0	TCP		192.168.3.131	43826	192.168.3.132	80	1:1000006	SYN Flood Dos
0	TCP		192.168.3.131	43824	192.168.3.132	80	1:1000006	SYN Flood Dos
0	TCP		192.168.3.131	43822	192.168.3.132	80	1:1000006	SYN Flood Dos
0	TCP		192.168.3.131	43820	192.168.3.132	80	1:1000006	SYN Flood Dos
0	TCP		192.168.3.131	43818	192.168.3.132	80	1:1000006	SYN Flood Dos

Şekil 3. 46. Snort Slowloris Alarm

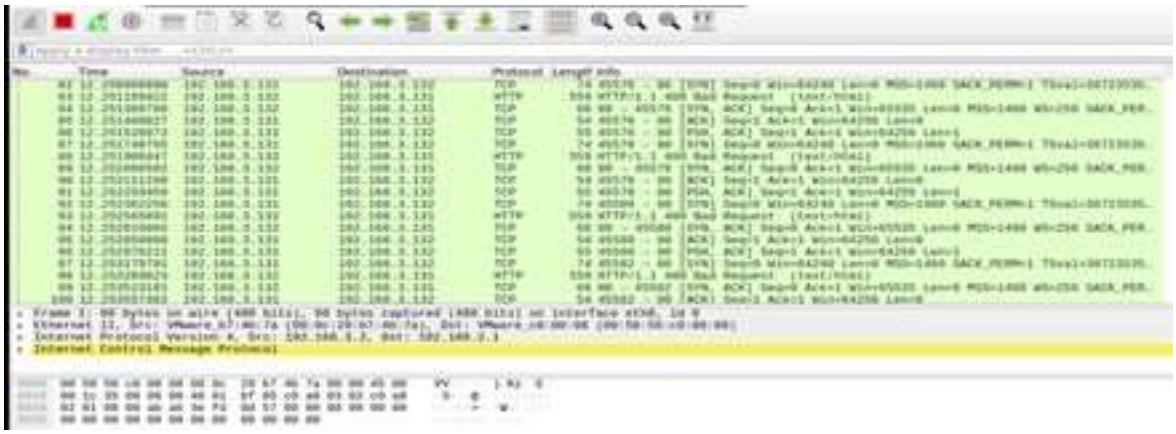
3.5.2.7. Xerxes Yalancı (Fake Session

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. (Penetration Testing, Penetration Testing Scanning, 2022)

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. 47. Xerxes uygulmasını github platformundan indirme

Şekil 3. 48. Xerxes Atak uygulanması



Şekil 3. 49. Wireshark Xerxes paket gönderme görüntüsü

Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
3	TCP	Unknown Traffic	192.168.3.132	80	192.168.3.131	45550	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
3	TCP	Unknown Traffic	192.168.3.132	80	192.168.3.131	45548	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
0	TCP		192.168.3.131	45550	192.168.3.132	80	1:1000006	SYN Flood Dos
3	TCP	Unknown Traffic	192.168.3.132	80	192.168.3.131	45546	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
0	TCP		192.168.3.131	45548	192.168.3.132	80	1:1000006	SYN Flood Dos
3	TCP	Unknown Traffic	192.168.3.132	80	192.168.3.131	45544	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
0	TCP		192.168.3.131	45546	192.168.3.132	80	1:1000006	SYN Flood Dos

Şekil 3. 50. Snort Xerxes alarmı

3.5.2.8. Golden Eye 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 3.51, Şekil 3.52, Şekil 3.53.

Şekil 3. 51.GoldenEye uygulamasını github platformundan indirme

Şekil 3. 52.GoldenEye Atak.

Şekil 3. 53. GoldenEye Snort Alarm.

4. BULGULAR ve YORUMLAR

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.

Oluşturulan ağ modeli çok temel düzeyde olup, yeni nesil yapay zekâ, makine öğrenmesi ve derin öğrenme yöntemleri ile saldırılarda güvenlik başarı oranları optimizasyon ile birlikte %96 seviyesini çıkartılabilir.

DDOS ve DOS ataklarına karşı alınabilecek önlemlerde 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.

Yeni ataklara karşı bulgularda 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.

5. SONUÇ ve ÖNERİLER

5.1. Sonuçlar

Günümüzde IDS (saldırı tespit sistemleri) ve IPS 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 kolay 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. Kullanıcıların siber güvenlik konusunda farkındalıklarını artırmak için sürekli olarak eğitim, oto kontrol, planlama ve kalite standartlarına uyumu hedef almak doğru bir yaklaşım olacaktır.

6. KAYNAKLAR

Ami, P., Hasan, A., (2012, Kasım). Seven Pharase Penetration Testing Model, International Journal of Computer Applications, Cilt 59, No.5, 0975-8887

Archive, http://archive.org, Erişim Tarihi:13.12.2022

Checkusernames, https://checkusernames.com, Erişim Tarihi: 13.12.2022

FreeBSD, FreeBSD Hakkında, https://www.freebsd.org/about.html Erişim Tarihi: 07.01.2022

Google, https://www.google.com , Erişim Tarihi: 13.12.2022

Mail-Archive, https://mail-archive.com, Erişim Tarihi: 13.12.2022

Maltego, https://maltego.com, Erişim Tarihi:13.12.2022

NMap, https://nmap.org, Erişim Tarihi:13.12.2022

Shodan, http://www.shodan.io, Erişim Tarihi: 13.12.2022

Wilhelm, T. (2010). Professional Penetration Testing, UK: Syngress, 219-257

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

Kali Linux, What is Kali Linux, https://www.kali.org/docs/introduction/what-is-kali-linux/ Erişim Tarihi: 01.07.2022

Pfsense, Getting-Started, https://www.Pfsense.org/getting-started/ Erişim Tarihi: 07.01.2022

Snort, Snort Community, https://www.snort.org/resources#documents Erişim Tarihi: 07.01.2022

Çavuş, M.F. ve Kurt, H.S.(2017).Kamu Kurumlarında Açık Kaynak Kodlu Yazılımların Kullanımı. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, 5(3).

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: 01.07.2022

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:07.01.2022

Kaspersky, DDoS Atağı Nedir, https://www.kaspersky.com.tr/resource-center/threats/ddos-attacks Erişim Tarihi: 07.01.2022

ISSA Turkey, DoS, DDoS Atakları, https://issatr.org/dosddos-ataklari/, Erişim Tarihi: 01.07.2022

Penetration Testing, Penetration Testing Scanning 101.3, https://www.secjuice.com/port-scanning-penetration-testing-part-three/ , Erişim Tarihi: 01.07.2022

Penetration Testing, Add Custum Header To Nicto Scan, https://www.cardinaleconcepts.com/add-custom-header-to-nikto-scan/ , Erişim Tarihi:01.07.2022

OSSTMM, Open Source Security Testing Metodology Manual, https://www.isecom.org/OSSTMM.3.pdf , Erişim Tarihi: 01.07.2022

VMware, “2019 Gartner Magic Quadrant'da Lider Oldu” https://www.vmware.com/content/microsites/learn/en/304750_REG.html Erişim Tarihi: 07.01.2022