Araştırma Makalesi / Research Article

Adli Bilişim Alanında Ağ Analizi

Nur Sena ATALAY, Şengül DOĞAN, Erhan AKBAL*, Türker TUNCER

Fırat Üniversitesi, Adli Bilişim Mühendisliği, Elazığ
(ORCID: 0000-0003-2053-7393)(ORCID:0000-0001-9677-5684)
(ORCID:0000-0002-5257-7560) (ORCID0000-0002-1425-4664)

Öz

Teknolojinin gelişimine bağlı olarak günümüzde aklımıza gelebilecek her alan internet ve ağ kullanımı ile gerçekleşmektedir. Günlük hayatımızın ayrılmaz bir parçası haline gelen ağ kullanımı, internet alışverişleri, veri aktarımları, iş hayatımız gibi birçok alanda internet üzerinden yapılmaktadır. İşlemlerin tamamı kişisel bilgiler, kredi kartı numaraları vb. kullanılarak kişisel bilgilerin paylaşılmaması ve güvenliğinin iyi sağlanması gereken olgular ile gerçekleşmektedir. Her geçen gün teknolojinin bir seviye daha ilerlemesi ile internet kullanıcılarının da sayısı artmaktadır. İnternet kullanımı olumlu yönleri olduğu kadar beraberinde bilgi güvenliği ve kişisel hayat ihlali gibi tehlikeleri de beraberinde getirmektedir. Büyüyen teknoloji ile bilgisayar korsanları, teknolojiyi ve onu ele geçirme yollarını her geçen gün biraz daha farklı teknikler ile gerçekleştirmektedir. Adli bilişim alanı, dijital ortamlarca iletilen verilerin, her türlü bilişim nesnesinin, mahkemede sayısal delil niteliği taşıyacak şekilde tanımlanması, saklanması, incelenmesi ve mahkemeye sunulması çalışmalarının bütünüdür. Adli bilişim alanında elde edilen bulgular çeşitli donanım ve yazılımlar ile gerçekleşmektedir fakat yazılım ve donanımlar her zaman yeterli olmamaktadır. Bu sebep ile çeşitli test ve analizlere ihtiyaç duyulmaktadır. Bu analizlerden biri de ağ analizidir. Ağ üzerinde gerçekleşen bir olayın aydınlatılması ve çeşitli delillerin elde edilebilmesi için ağ analizi kullanılmaktadır. Günümüzde ağ analizi yapmak ve ağ trafiği dinlemek için çeşitli programlar kullanılmaktadır. Bu çalışmada, adli bilişim alanında olayların aydınlatılmasında ağ analizinin kullanımı ve öneminden bahsedilmiş, ağ analizin de kullanılan programlardan olan Nmap, Zenmap ve NetworkMiner programları incelenerek çeşitli uygulamalara yer verilmiş ve programlar arası yetenek karşılaştırması yapılarak elde edilen bulgular görselleştirilerek sunulmuştur.

Anahtar kelimeler: Adli Bilişim, Ağ analizi, Ağ güvenliği, Nmap, NetworkMiner, Zenmap.

Network Analysis in Digital Forensics

Abstract

Depending on the development of technology, nowadays, every area that may come to our mind is realized through internet and network usage Networking, which is an integral part of our daily life, is done over the internet in many areas such as internet shopping, data transfer and business life. All transactions are performed using personal information, credit card numbers, etc., so as not to share personal information and to provide a good security. With the advancement of technology, the number of internet users is increasing. information security and personal life violations are increasing with the widespread use of the Internet. Growing technology and hackers, technology and ways to obtain it is performing every day with a little different technique. The digital forensic computing area is the collection of data that is transmitted by digital media in a way to be defined as a digital evidence in the court, storing, examining and presenting to the court. Findings in the field of forensic information are made by various hardware and software. However, software and hardware are not always sufficient. Therefore, various tests and analyzes are required. One of these analyzes is network analysis. Network analysis is used to illuminate an event on the network and to obtain various evidence. Today, various programs are used for network analysis and network traffic. In this study, the use and importance of the network analysis in the field of forensic informatics is mentioned and various programs are used by analyzing the Nmap, Zenmap and NetworkMiner programs which are used in network analysis.

Keywords: Digital Forensics, Network analysis, Network security, Nmap, NetworkMiner, Zenmap.

*Sorumlu yazar: erhanakbal@firat.edu.tr
Geliş Tarihi: 06.11.2018, Kabul Tarihi: 18.03.2019

1. Giriş

Günümüzde aklımıza gelebilecek her alan internet kullanımı ile gerçekleşmektedir. İnternet alışverişleri, veri aktarımı, iş yerleri, okullar vb. birçok alanda veri alışverişi internet üzerinden yapılmaktadır. İşlemlerin tamamı kişisel bilgiler, kredi kartı numaraları vb. kullanılarak kişisel bilgilerin paylaşılmaması ve güvenliğinin iyi sağlanması gereken olgular ile gerçekleşmektedir. İnternet kullanıcılarının günden güne artan sayısı ile internet üzerinden iletilen her veri, başka bir kişinin kötü niyetli bir şekilde zarar görmesinden dolayı tehdit altındadır. Sistem ağına gönderilen verilere güvenlik sağlamak için ağ güvenliği yetersiz kalmaktadır. Büyüyen teknoloji ile bilgisayar korsanları, teknolojiyi ve onu ele geçirme yollarını her geçen gün biraz daha farklı teknikler ile gerçekleştirmektedir. Adli Bilişim, elektronik ortamda muhafaza edilen veya bu ortamlarca iletilen ses, görüntü, veri, bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal delil niteliği taşıyacak şekilde tanımlanması, saklanması, incelenmesi ve mahkemeye sunulması çalışmalarının bütünüdür. Adli bilişim de elektronik ortamda bulunan bilgilerin uygun yazılımlar ve donanımlar ile delile dönüştürme süreci, hukuki boyuttan daha çok teknik ve uzmanlık isteyen bir iştir. Sürekli gelişen sistemler, yeni donanımlar, yazılımlar ve sosyal medya araçları, artan kullanıcı sayısına bağlı olarak sabit disklerin kopyalarını almak önemli bulguların sonuca ulaşmasında yeterli olmayabilmektedir. Bu nedenden dolayı çeşitli analizlere ihtiyaç duyulmaktadır. Bu analizlerden önemli olanlarından biri de ağ analizidir. Ağ üzerinde gerçekleşen bir olayın aydınlatılması ve çeşitli delillerin elde edilebilmesi için ağ analizi yöntemi kullanılmaktadır. Günümüzde ağ analizi yapmak ve ağ trafiği dinlemek için çeşitli programlar kullanılmaktadır. Programların kullanım amacı genel olarak ağ trafiğini dinlemek, giden ve gelen ağ paketlerini yakalayarak ağ analizi yapmaktır. Bu çalışmada, adli bilişim alanında olayların aydınlatılmasında önemli bir yeri olan ağ analizinin yapılması için kullanılan Nmap, Zenmap ve NetworkMiner programları incelenecektir ve programlar kullanılarak çeşitli uygulamalara yer verilecektir.

Ağ; bilgisayarlar, sunucular, ağ cihazları gibi bir grup aygıtın topluluğunun birbirleri arasında veri alışverişi ve haberleşmesine imkân sağlayan yapı olarak adlandırılabilir [1]. Bir ağın en mükemmel örneği, tüm dünyada milyonlarca insanı birbirine bağlayan internet olarak verilebilir. Bir ağ, fiziksel veya kablosuz bağlantılarla bağlanmış bir dizi farklı bilgisayar sisteminden oluşur. Ölçek, temel çevre birimlerini dünya çapında bulunan büyük veri merkezleri ya da tek bir bilgisayar olabilir. Kapsamı ne olursa olsun, tüm ağlar bilgisayarların veya bireylerin bilgi ve kaynakları birbirleri arasında paylaşmalarına olanak sağlar. Bilgisayar ağları faydalı bir takım amaçlar sunmaktadır. Amaçları arasında e-posta, anlık mesajlaşma, yazıcılar ve giriş cihazları gibi paylaşılan donanım iletişimleri; paylaşılan depolama aygıtlarının kullanımı yoluyla veri aktarımı da vardır. Ağ yapısı, günlük hayatımızın her alanında karşımıza çıkmaktadır ve haliyle verilerimizin bütünlüğü açısından ağ güvenliği çok iyi sağlanmalıdır. Ağ güvenliği, tüm ağ trafiği de dâhil olmak üzere varlıklarının güvenliğini garanti eden bir kuruluşun stratejisidir. Hem yazılım hem donanım teknolojilerini içerir. Ağa erişim, geniş bir tehdit yelpazesini hedefleyen etkin ağ güvenliği tarafından yönetilir ve daha sonra bunların ağa yayılmasını veya ağa girmesini engeller. En etkili ağ güvenliği, ağa erişimini yönetmekle sağlanmaktadır. Ağ güvenliği, ağ üzerinde birden çok savunma katmanını birleştirir. Her ağ güvenlik katmanı, kendi politikalarını ve denetimlerini uygular. Yetkili kullanıcılar ağ kaynaklarına erişebilir, ancak kötü niyetli aktörlerin istismar ve tehditler gerçekleştirmesi engellenir. Ağ erişim kontrolü sürecine göre, her kullanıcının her ağa bağlantısına erişimi olmamalıdır. Potansiyel saldırganlardan korunmak için, her bir kullanıcıyı ve her bir cihazı tanımak gerekir. Ardından güvenlik politikası uygulanabilir. Uyumlu olmayan uç nokta cihazları engellenebilir veya sadece sınırlı erişim bağlantısı sağlanabilir. Ağ güvenliği türlerine örnek olarak antivirüs ve antimalware yazılımları, uygulama güvenliği veri kaybını önleme (DLP), e-posta güvenliği, güvenlik duvarları, mobil cihaz güvenliği, ağ segmentasyonu, güvenlik bilgisi ve etkinlik yönetimi (SIEM),web güvenliği, kablosuz ağ güvenliği, ağ erişim kontrolü (NAC) örnek olarak verilebilir. Sistem ve ağ teknolojisi, çok çeşitli uygulamalar için önemli bir teknolojidir.

Güvenlik gereksinimlerinin karmaşıklığını yönetmek için genel olarak kullanılan bir yöntem olduğunu tanımlamak zordur. Bir bilgisayar korsanı tarafından bir hedef kaynak belirlenebilir, verileri alıp şifresini çözecek ve bir takım mesajı tekrar gönderilebilir. Ağın güvenliğini sağlamak, bilgisayarları güvenli hale getirmek ve mesajları şifrelemek kadar önemlidir. Güvenli bir ağ geliştirirken gizlilik ve bütünlük esas alınarak hareket edilmelidir. Gizlilik faktörüne göre, kimliği doğrulanmayan tarafın

verileri inceleyemeyeceği anlamına gelir. Bütünlük faktörüne göre ise alıcı tarafından alınan verilerin değişmediği veya gönderen tarafından gönderildikten sonra değiştirilmediği esas alınarak hareket edilir. Ağ saldırı türlerinde ağ performansı, kontrolsüz trafik, virüsler vb. gibi faktörler için bir neden olabilecek bazı temel saldırı sınıflarını vardır [2]. Saldırılar iki türde kategorize olmaktadır. Bunlardan ilki olarak pasif saldırı türü örnek verilebilir. Bir ağ saldırıcısı, ağ üzerinden geçen verileri engellediğinde "Pasif" saldırı olarak adlandırılmaktadır. Bir saldırganın ağın normal çalışmasını kesintiye uğratmak amacıyla kötü amaçlı komutlarını başlattığı saldırı türü ise "Aktif" saldırı olarak adlandırılmaktadır. Tablo 1 ve Tablo 2 ile ağ saldırı türleri detaylı olarak verilmiştir.

Tablo 1. Aktif saldırı türleri [1-6].

Aktif Saldırı	**Spoofing Attack**	Kötü amaçlı taraf, ağ üzerindeki ana bilgisayarlara yönelik saldırıları başlatmak, veri çalmak, kötü amaçlı yazılım yaymak veya erişim denetimlerini atlamak için ağ üzerindeki başka bir aygıtı veya kullanıcıyı taklit ettiğinde ortaya çıkan saldırı türüdür. IP Spoofing saldırısı, bir ağ üzerinden farklı bir sisteme erişilmek istenildiğinde, erişimin sağlandığı IP adresinin sunucu üzerinde farklılık göstermesi ile oluşmaktadır. Kullanılan bu yöntem ile karşı hedefe erişim kısıtlaması olmayan bir aygıtın IP adres bilgisi kullanılarak sisteme erişim sağlanabilir. Sisteme erişimi olan aygıtların IP adreslerinin keşfi; nmap ve zenmap gibi ağ keşif ve analiz programları ile elde edilebilmektedir.
	Modification Attack	Modifikasyon saldırısı anlamına gelmektedir. Kötü amaçlı olarak yönlendirme yolunda bazı değişiklikler yaptığında, gönderen mesajı uzun yoldan gönderir. Bu saldırı, gönderen ve alıcı arasında iletişimin gecikmesine neden olmaktadır. Paketlerin yönlendirilmesi amacına yönelik olarak yapılan bu saldırı türünün gerçekleşmesinde, nmap, networkminer ve zenmap gibi ağ trafiği dinleme programları kullanılarak, paket dinleme giden ve gelen paketlerin sayısının bilgisi gibi verilerin elde edilmesi saldırıyı kolaylaştırmaktadır.
	Wormhole Attack	Bu saldırıya solucan deliği ya da tünel saldırısı da denilmektedir. Bu saldırıda, bir saldırgan bir noktada bir paket alır ve ağdaki başka bir kötü amaçlı diğer bir bağlantıya yönlendirir. NetworkMiner gibi paket yakalama programları ile paketler hakkında elde edilen bilgiler saldırının gerçekleşmesinde kullanılabilmektedir.
	Denial of Services Attack	Hizmet reddi saldırısında, kötü amaçlı saldırganın iletiyi, ağda ki diğer bir bağlantıya göndermesi ve ağın bant genişliğini tüketmesi ile gerçekleşmektedir. Saldırının asıl amacı, ağı fazla bağlantı isteğiyle meşgul etmektir. Eğer kimliği doğrulanmamış bağlantıdan bir mesaj gelirse, mesajı almayacaktır. Bunun nedeni meşgul ve yeni başlayan alıcı yanıtını beklemek zorunda olmasıdır.
	Sinkhole Attack	Sinkhole, baz istasyonunun tam ve doğru bilgi elde etmesini engelleyen bir servis saldırısıdır. Bu saldırıda, bir bağlantı, tüm komşu bağlantılardan verileri kendine çekmeye çalışmaktadır. Saldırı öncesi doğru bilginin elde edilmesinde ağ trafiği dinleme ve analiz etme programları kullanılabilmektedir.

Tablo 2. Pasif saldırı türleri

Pasif Saldırı	**Traffic Analysis**	Trafik analizi saldırısında, saldırgan gönderen ve alıcı arasındaki iletişim yolunu algılamaya çalışır. Saldırgan, gönderenin ve alıcının yolundan geçen veri miktarını bulabilmektedir. Trafik analizinde verilerde bir değişiklik bulunmamakta ve veri bütünlüğü sabit kalmaktadır. Trafik analizi saldırılarında nmap, zenmap ve networkminer programları ile ağ trafiği dinleme, analiz etme ve veri elde etme işlemleri ile saldırının yapılması kolaylaşmaktadır.
	Eavesdropping	Dinleme olarak adlandırılan bu saldırı türü, mobil ağ üzerinde meydana gelen pasif bir saldırıdır. Bu saldırının temel amacı, iletişim sırasında olan gizli verileri elde etmektir. Nmap ve zenmap programları ile trafik dinleme ve veri elde etme işleminde saldırının gerçekleşmesine yardımcı olmaktadır.
	Monitoring	İzleme olarak adlandırılan bu saldırı türünde, saldırgan gizli verileri okuyabilir fakat veriler üzerinde herhangi bir düzenleme yapamaz ve veri bütünlüğü sabit kalır. Ağ izleme ve veri elde etme aşamasında networkminer, nmap ve zenmap gibi analiz programları kullanılabilmektedir.

2. Adli bilişim alanında ağ analizinin önemi

Adli bilişim alanında bulunan kanıtlar, işlenen suçun türüne bağlı olarak değişmektedir. Örneğin, bir ceza davasında, cinayetlerde, çocuk istismarında, mali dolandırıcılıkta ya da zimmete para geçirme gibi suçlara ilişkin kayıtlardan elde edilen belgeler mahkemelerce ve resmi makamlarca kanıt olarak kabul görmektedir. Bilgisayar bağlantılı suçlarda, sistemin farklı bileşenleri tarafından toplanan veriler kanıt niteliği taşımaktadır. Veri bir suç işlenene kadar kanıt haline gelmez ve bu veriler suçun aydınlatılmasında ipuçlarını bulmak için kullanılmaktadır. Bu nedenle, bilişim alanında elde edilen veriler aslında potansiyel kanıt niteliği taşımaktadır. Bilgisayarlarda ve ağ bileşenlerinde birçok potansiyel kanıt kaynağı vardır. Dosyalar, resimler, uygulamalar, programlar vb. veriler potansiyel kanıtlara örnek olarak verilebilir. Daha derinlemesine incelendiğinde; internet vb. geçmiş kayıtları, önbellek bilgileri, yedeklemeler veya etkinlik günlüklerini içerebilen gizli uygulama dosyaları gibi veriler potansiyel kanıt niteliği taşıyan verilerdir. Dijital bir aygıt üzerinden kanıt elde etme aşamasında, şifreleme, gizleme vb. etkinlikler ile kanıtların elde edilmesi zorlaştırılmış olabilmektedir. Olayın aydınlatılması ve kanıtların elde edilmesi için özel becerilere sahip kişiler tarafından incelenmesi gerekmektedir. Adli bilişim uzmanları, adli soruşturmayı başarılı bir şekilde yürütmek için gerekli becerilerle özel olarak eğitilmiştir. Bir adli bilişim uzmanı, bir dedektifin araştırma becerilerine, bir avukatın hukuki becerilerine ve suçlunun hesaplama becerilerine sahip olmaktadır. Günlük hayatımızda teknolojinin de gelişimine bağlı olarak internet kullanımı, son on yılda büyük ölçüde artmıştır. İnternet ve ağ kullanımı günlük hayatımızın hemen her alanında karşımıza çıkan, birçok kişisel ve iş alanında gerçekleşen aktivitelerde yaygın olarak kullanılan bir yapıdır. İnternet kullanım sayısı arttıkça, veri hırsızlığı, kimlik hırsızlığı, vb. gibi yasadışı faaliyetlerin sayısı da katlanarak artmaktadır. Adli Bilişim, bilgisayar sistemlerinden, ağlardan, iletişim akışlarından (kablolu ve kablosuz) ve depolama medyasından bir mahkemede kabul edilebilir bir şekilde veri toplanması ve analiz edilmesi ile ilgili çalışmalar bütününü kapsamaktadır. Adli bilişim alanında elde edilen bulgular çeşitli donanım ve yazılımlar ile gerçekleşmektedir fakat yazılım ve donanımlar her zaman yeterli olmamaktadır. Bu sebep ile çeşitli test ve analizlere ihtiyaç duyulmaktadır. Bu analizlerden biri de ağ analizidir. Ağ üzerinde gerçekleşen bir olayın aydınlatılması ve çeşitli delillerin elde edilebilmesi için ağ analizi kullanılmaktadır [3]. Bu alanda ağ analizinin önemi, bir mahkemede güvenlik saldırılarının kaynağı hakkında kanıtsal bilgi elde etmek amacıyla ağ olaylarının yakalanması, kaydedilmesi ve analizi olarak tanımlanabilir.

3. Nmap ve zenmap analiz parametreleri

Ağ dinlemesi, ağ üzerinden veri elde edilmesi ve incelemesi gibi ağ üzerine yapılan çeşitli analizler, yazılımlar ile gerçekleşmektedir. Bunlara örnek olarak NetworkMiner, Nmap ve Zenmap programları verilebilir. NetworkMiner programı genel olarak kaydedilmiş ağ dinleme kayıtları olan pcap uzantılı dosyaları analiz etmek amacıyla kullanılmaktadır. Nmap ve Zenmap programları, ağ dinleme, tarama ve veri elde etme amacıyla kullanılan programlardır. Nmap ve Zenmap programları ağ tarama ve analiz işlemini çeşitli parametreler ile gerçekleştirmektedir. Kullandıkları parametreler Tablo 3 ile detaylı olarak verilmiştir.

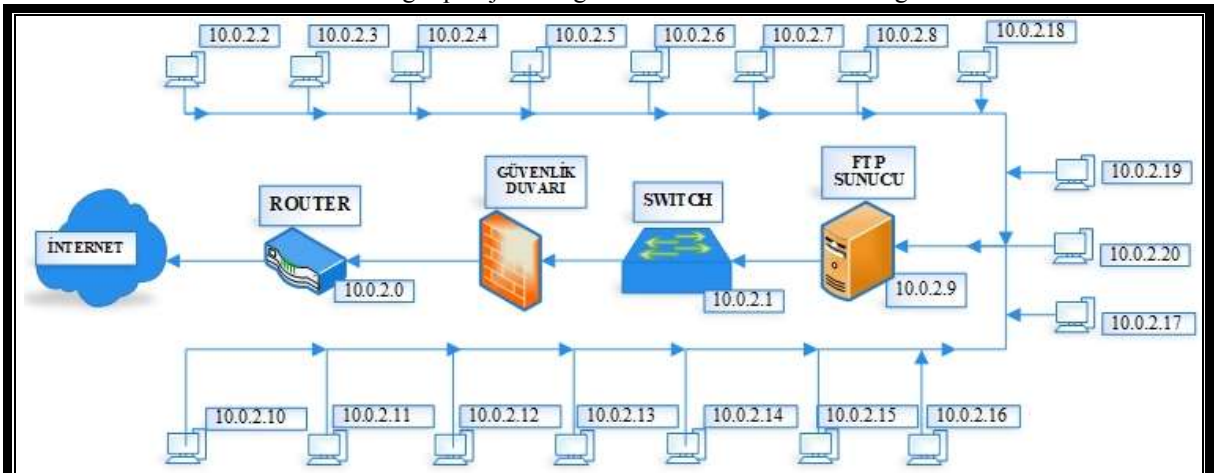
Tablo 3. Nmap ve Zenmap programları ağ tarama ve analiz etme parametreleri

TEMEL TARAMA TEKNİKLERİ	
nmap [target]	Tek bir hedefi tarama amacıyla kullanılan parametredir.
nmap [target1,target2,etc]	Birden çok hedefi tarama amacıyla kullanılan parametredir.
nmap -iL [list.txt]	Hedeflerin bir listesini çıkarma amacıyla kullanılan parametredir.
nmap [IP address/cdir]	Ağın bir alt ağını tarama amacıyla kullanılan parametredir.
nmap -iR [number]	Rasgele olarak host tarama amacıyla kullanılan parametredir.
nmap [targets] –exclude [targets]	Hedef filtrelemesi yaparak, tarama yapılmasının istenmediği hedefi ya da hedef aralığını belirtmek amacıyla kullanılan parametredir.
nmap [targets] –excludefile [list.txt]	Hedef filtrelemesi yaparak, tarama yapılmasının istenmediği hedefi ya da hedef aralığını bir liste kullanarak belirtmek amacıyla kullanılan parametredir.
nmap -6 [target]	IPv6 türünde hedefi tarama amacıyla kullanılan parametredir.
AĞ KEŞİFİ PARAMETRELERİ	
nmap -sP [target]	Ping taraması yapmak amacıyla kullanılan tarama parametresidir.
nmap -PS [target]	SYN bayraklı paketler ile TCP ping tarama işlemi için kullanmaktadır. Hedefe SYN bayraklı bir paket gönderilir ve hedeften RST ya da SYN/ACK bayraklı paketler beklenir. Eğer bu paketlerden biri gelirse hedefin aktif olduğu anlamına gelmektedir.
nmap -PA [target]	ACK bayraklı paketler ile TCP ping tarama işlemi için kullanmaktadır.
nmap -PU [target]	UDP ping tarama işlemi için kullanmaktadır.
nmap -PO [target]	IP protokolü ping taraması yapmak amacıyla kullanılan tarama parametresidir.
nmap -PR [target]	ARP ping taraması yapmak amacıyla kullanılan tarama parametresidir.
nmap –system-dns [target]	DNS araması yapmak amacıyla kullanılan parametredir.
nmap –dns-servers [servers] [target]	DNS sunucularını manuel olarak belirtmek amacıyla kullanılan parametredir.
nmap -sL [targets]	Ana makinelere ait bir listesi oluşturmak amacıyla kullanılan parametredir.
GÜVENLİK DUVARI KEŞİF PARAMETRELER	
nmap -f [target]	Parça paketleri tarama amacıyla kullanılan parametredir.
nmap -sI [zombie] [target]	Idle zombi taraması amacıyla kullanılan parametredir.
VERSİYON KEŞİF PARAMETRELERİ	
nmap -O [target]	İşletim sistemi tespiti amacıyla kullanılan parametredir.
nmap -sV [target]	Servis sürümü algılama amacıyla kullanılan parametredir.
nmap -sR [target]	RPC taraması amacıyla kullanılan parametredir.
ÇIKTI PARAMETRELERİ	
nmap -oN [scan.txt] [target]	Analiz sonucu elde edilen verilerin bir çıktısını txt formatı uzantısı ile metin dosyası olarak kaydedebilmek amacıyla kullanılan parametredir.
nmap -oX [scan.xml] [target]	Analiz sonucu elde edilen verilerin bir çıktısını xml formatı uzantısı kaydedebilmek amacıyla kullanılan parametredir.
nmap -oA [path/filename] [target]	Analiz sonucu elde edilen verilerin bir çıktısını desteklenen tüm dosya formatlarına uygun olarak kaydedebilmek amacıyla kullanılan parametredir.

4. Nmap, zenmap ve networkminer programları uygulama yöntemi

Adli bilişim alanında, olayların aydınlatılmasında kullanılan analizler arasında ağ analizi önemli bir yer almaktadır. Ağ saldırıları için elde edilmesi gereken çeşitli bilgiler genel olarak ağ trafiği dinlemesi ve analizi ile gerçekleşmektedir. Ddos, aktif ağ saldırıları, pasif ağ saldırıları gibi saldırıların gerçekleştirilebilmesi için hedef aygıt ile alakalı çeşitli bilgilere erişmek gerekmektedir. Tablo 4 ile erişilmesi gereken bu bilgilerden bazıları "Aranan Veriler" başlığı adı altında verilmiştir. Aynı zamanda Tablo 4 ile içerisinde bilgisayar, sunucu, router ve switch aygıtlarından oluşan örnek bir ağ topolojisi gösterilmiştir.

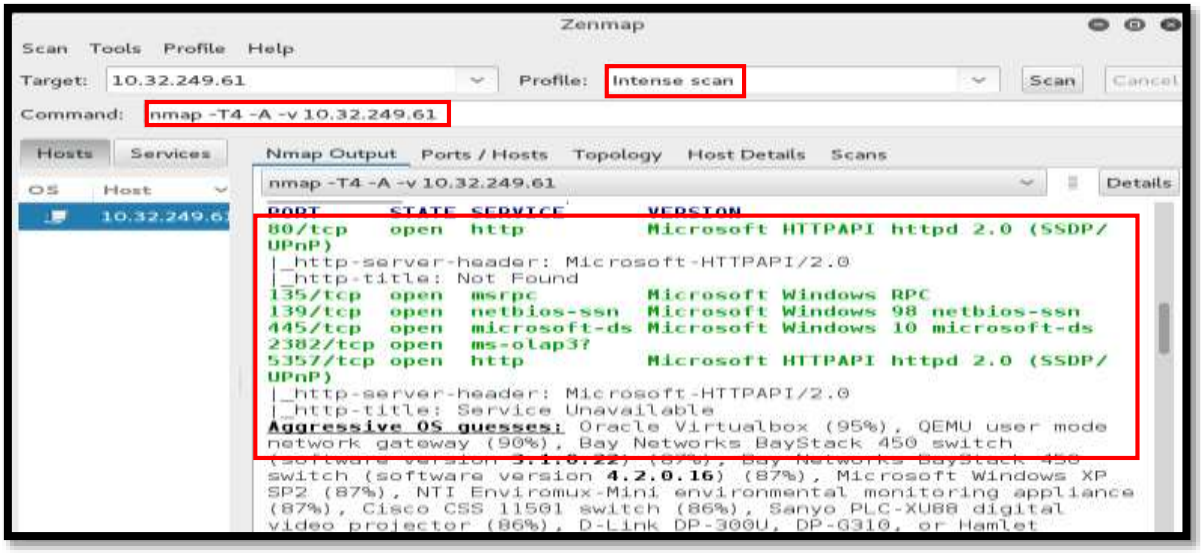
Tablo 4. Ağ topolojisi ve ağ üzerinde aranan verilerin bilgisi



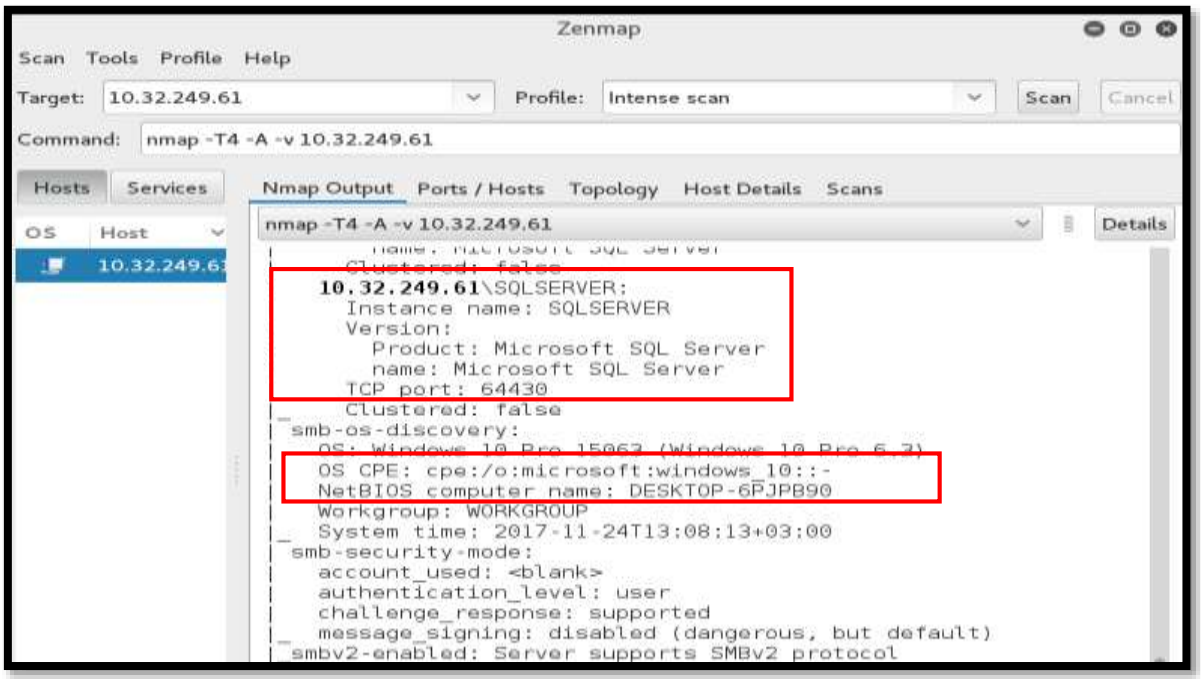
ARANAN VERİLER

1. Port, Servis ve Versiyon Bilgisi
2. Protokol Bilgisi
3. Sistem Bilgisi
   - Gelen Paket Bilgisi
   - Giden Paket Bilgisi
4. MAC – IP Adres Bilgisi
5. TCP – UDP Protokol Bilgisi
6. Ağ Aygıt Listesi
7. Tüm Ağ Pcap Dosyası Analizi
   - 7.1. Kullanıcı Adı ve Şifre Bilgisi
   - 7.2. Resim, Doküman vb. Belge Bilgisi
   - 7.3. İnternet Geçmişi Bilgisi
8. Sunucu Bilgisi

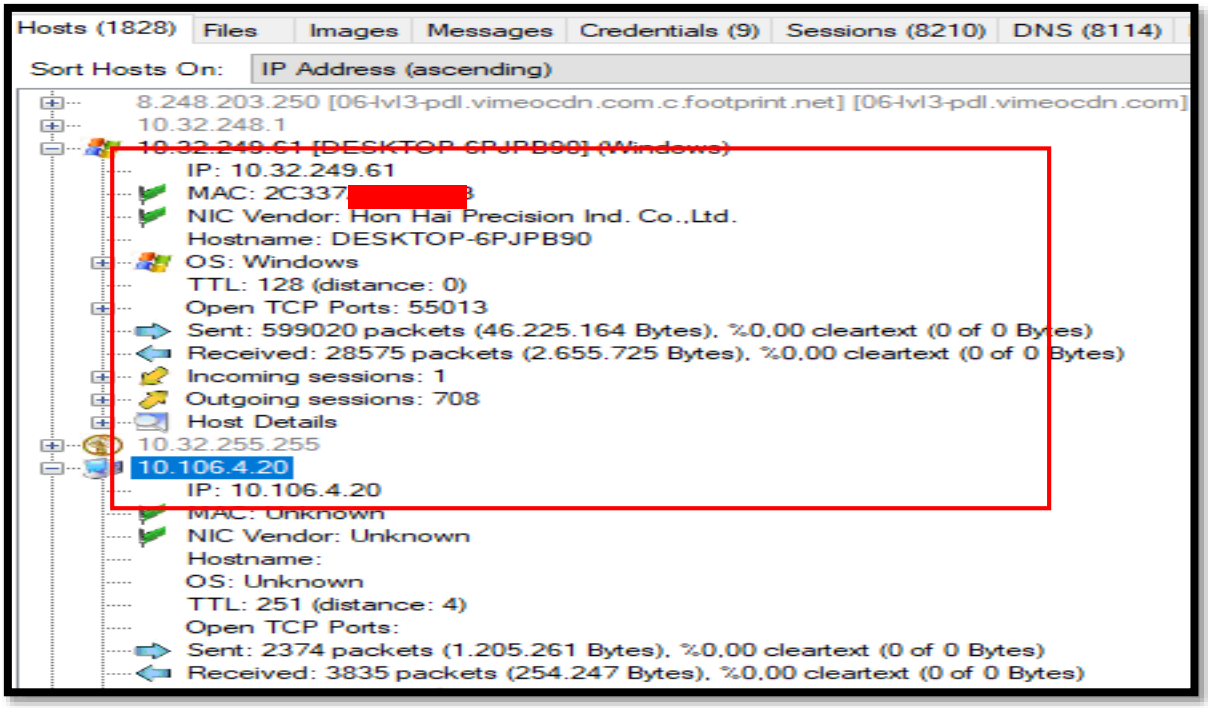
Bu çalışmada, ağ analizi ve taraması amacıyla kullanılan Nmap, Zenmap ve NetworkMiner programları kullanılarak Tablo 4 ile verilen örnek ağ topolojisi üzerinde ve farklı ağ topolojileri üzerinde ağ analiz uygulamalarına yer verilmiş ve aranan verilere ulaşılmaya çalışılmıştır. Uygulamada ilk olarak Zenmap programı ile **nmap –T4 –A –v** parametresini kullanarak hedef adrese "Intense" taraması yapılarak [4] hedef adrese yönelik olarak detaylı bilgi elde edilmiştir. Elde edilen sonuçlar Şekil 1 ve Şekil 2 ile verilmiştir. Elde edilen sonuçlar arasında hedef aygıt ile alakalı olarak port durum, servis, sürüm, bilgisayar ismi, işletim sistemi ve server bilgisi yer almaktadır. Programların kullanımına yönelik olarak yapılan ikinci uygulamada NetworkMiner programı kullanılarak hedef aygıt ile alakalı Mac adresi, IP adresi, işletim sistemi, alınan ve gönderilen paketlerin durum bilgisi gibi bilgilere ulaşılmıştır. Elde edilen sonuçlar Şekil 3'de gösterilmiştir.



Şekil 1. Zenmap programı ile Intense taraması sonucu port, servis ve versiyon bilgileri

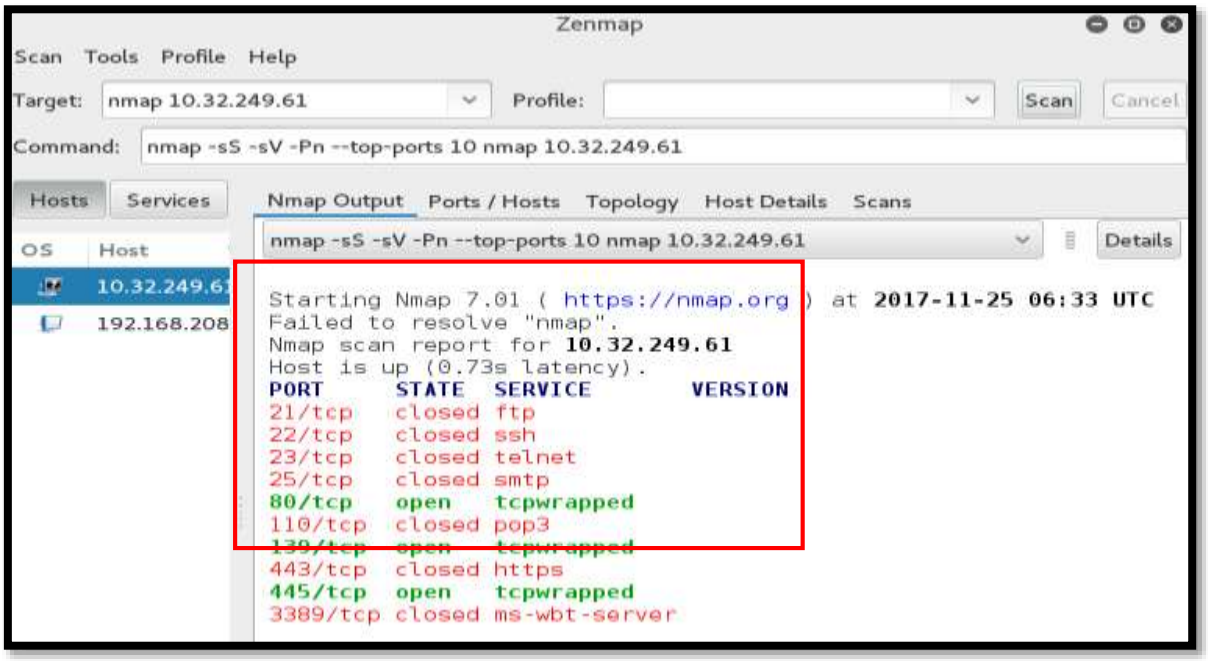


Şekil 2. Zenmap programı ile Intense taraması sonucu işletim sistemi, bilgisayar ismi ve sunucu bilgileri



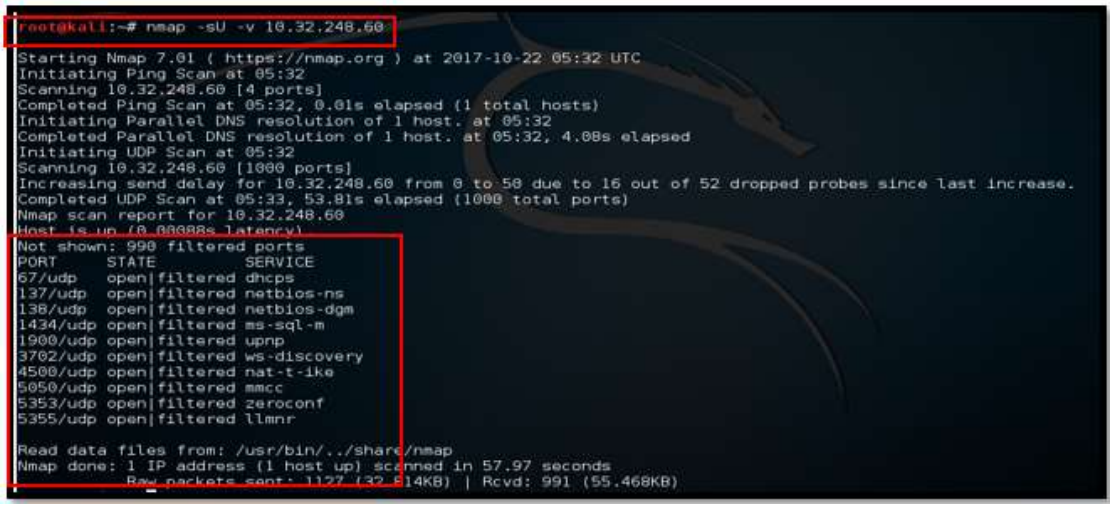
Şekil 3. NetworkMiner inceleme programı ile yapılan tarama sonucuna göre elde edilen bulgular

Ağ saldırılarında, karşı hedefe sızabilmek için hedef aygıt hakkında bilinmesi gereken önemli bilgilerden biri de port durum ve servis bilgisidir. Ağ analiz programları ile yapılan uygulamada bir sonraki aşama olarak, en çok kullanılan 10 port bilgisini elde etmek amacıyla Zenmap programı ile **nmap -sS -sV-Pn –top-ports 10 nmap[ip adres]** parametresini kullanarak hedef adrese port taraması yapılmıştır. Tarama sonucu hedef adrese yönelik olarak en çok kullanılan 10 port ve detaylı port durum bilgisi elde edilmiştir. Elde edilen sonuçlar Şekil 4 ile gösterilmiştir. Tarama sonuçlarına göre tcp 21-22-23-25-80-110-139-443-445-3389 portları hakkında port açık ve kapalılığı gibi durum bilgisi ve servis bilgisi elde edilmiştir.



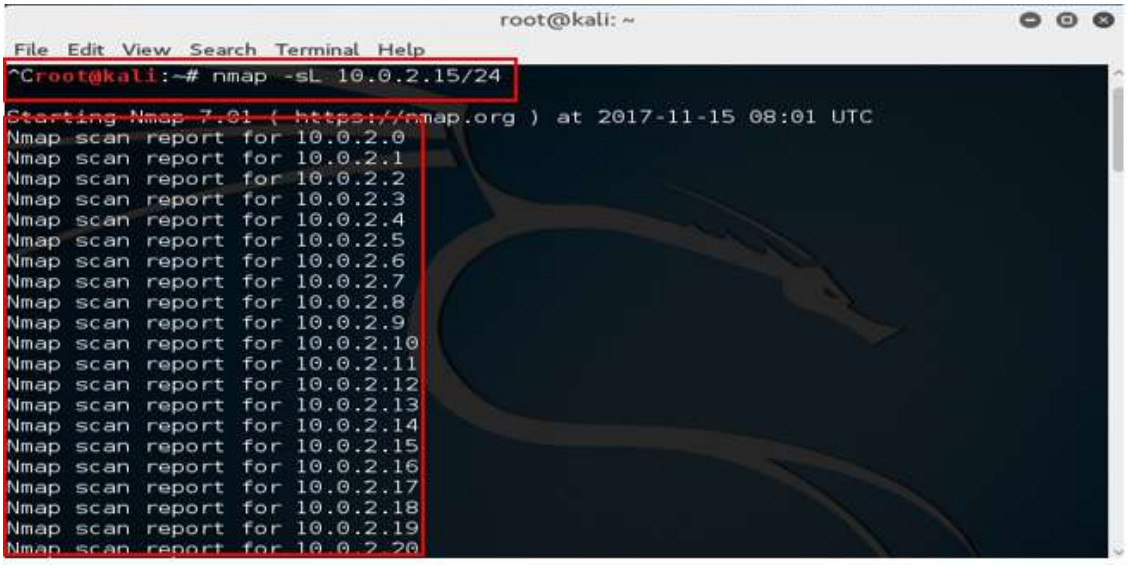
Şekil 4. Zenmap programı ile en çok kullanılan 10 port ve detaylı durum bilgisi

Bazı ağ saldırılarında karşı hedef ile alakalı bilinmesi gereken diğer önemli bilgilerden biride protokol bilgisidir. Tcp ve Udp protokolleri farklı çalışma yöntemlerine sahiptir. Tcp protokolü verinin karşı hedefe ulaşıp ulaşmadığı "Threeway Handshake" denilen yöntem ile kontrol ederken, Udp protokolü veri iletiminin yapılıp yapılmadığını kontrol etmez. Udp protokolü ile yapılan veri iletiminde kontrol durumu olamamasında dolayı, Udp Flood saldırılarında karşı hedefe rastgele çok fazla sayıda Udp paketi gönderilmesiyle dos saldırısı yapılabilmektedir. Karşı hedefe yapılan ağ saldırılarında öğrenilmesi gereken önemli bilgilerin başında protokol bilgisi gelmektedir. Uygulamanın bu aşamasında, Nmap ağ analizi programı ile **nmap –Su –v [ip adres]** parametresi kullanılarak Udp port taraması yapılmıştır [5]. Elde edilen sonuçlar Şekil 5 ile gösterilmiştir. Elde edilen sonuçlara göre UDP portlarının durum ve servis bilgilerine erişilmiştir.



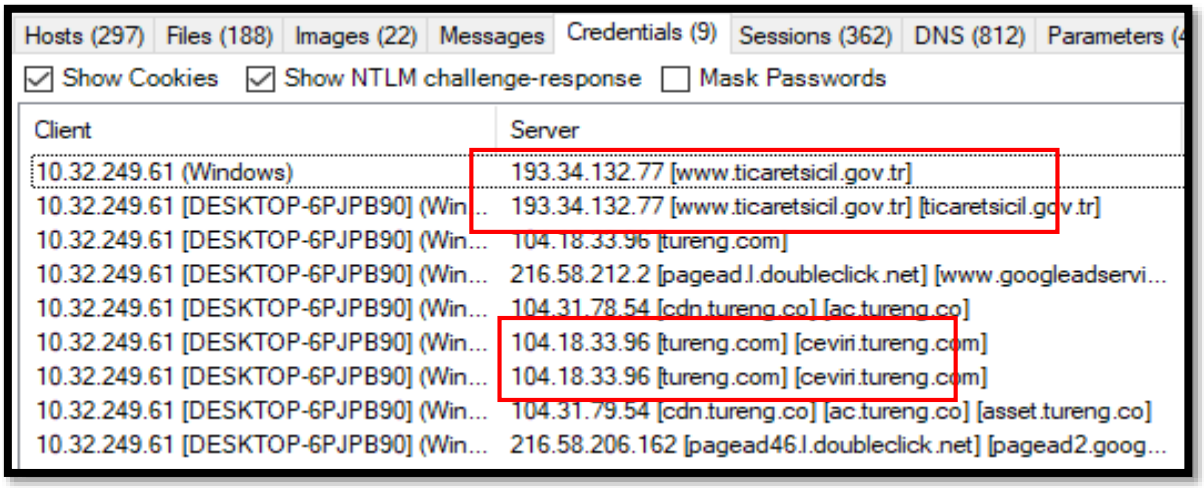
Şekil 5. Nmap programı ile UDP portları durum ve servis bilgileri

Ağ saldırılarında, hedef ağın içerisinde bulunduğu ağ yapısında birden fazla aygıt bulunabilmektedir. Saldırının yapılacağı hedef ağ üzerinde yapılan sunucu ve istemci keşfetme analizi ile karşı hedef üzerinde bulunan aygıtlara ait Ip bilgilerine ulaşılabilmektedir. Ulaşılan bilgiler doğrultusunda, saldırı yapılacak hedef aygıt ile alakalı hedef ip aralığına ulaşılabilmektedir. Uygulamanın bu aşamasında, Nmap ağ analizi programı ile **nmap –SL [ip adres]** parametresi kullanılarak sunucu ve istemci keşfetme yeteneği ile hedef adreslerin bir listesi çıkarılmıştır. Hedef ağ üzerinde bulunan bilgisayarların ip adres bilgilerine ulaşılmıştır. Elde edilen sonuçlar Şekil 6 ile gösterilmiştir.

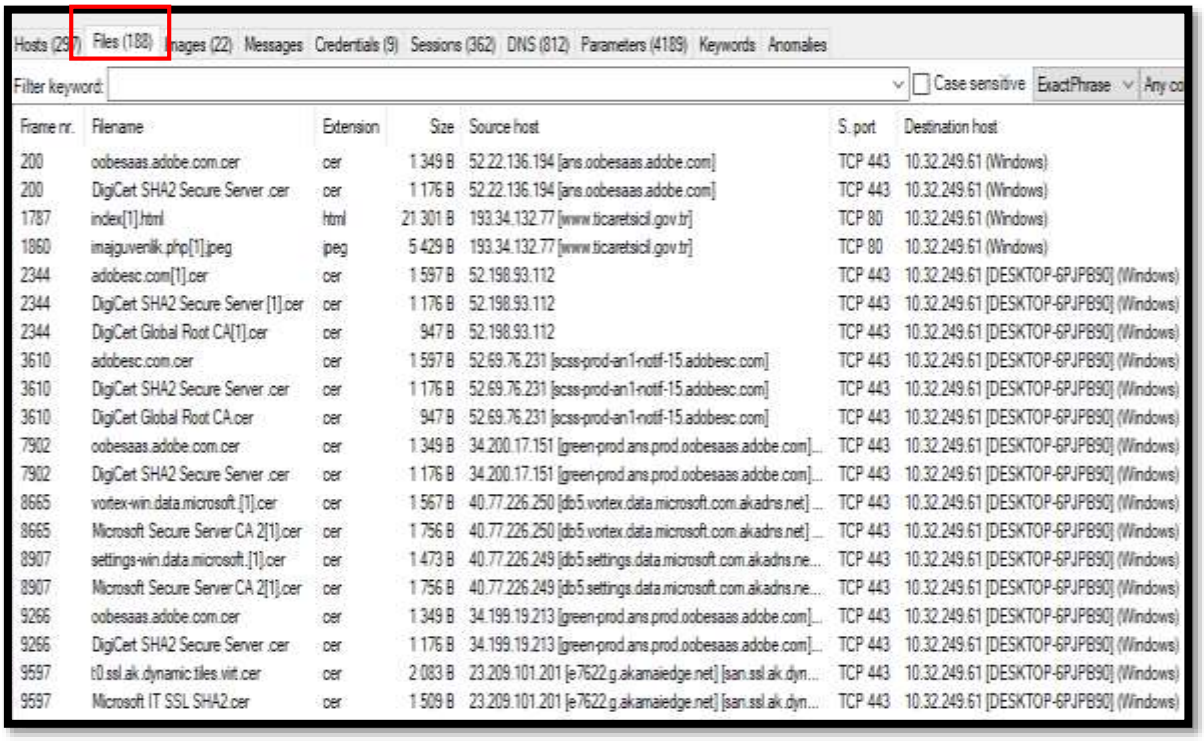


Şekil 6. Nmap programı ile hedef ağ üzerinde bulunan aygıtların keşfi

Hayatımızın hemen her alanında kullandığımız en büyük ağ yapılarından olan internet ağı günlük işlerimizin birçoğunda kullandığımız ve zamanımızın büyük bir kısmını geçirdiğimiz bir yapıdır. Günlük yaşamın hemen her alanında karşımıza çıkan ağ yapısının, adli bilişim alanında olayların aydınlatılmasında büyük bir önemi vardır. NetworkMiner inceleme ve analiz programı ile ağ analizi sonucu kaydedilen pcap uzantılı ağ dosyalarının inceleme ve analizi yapılabilmektedir [6]. Adli bilişim alanında, adli kopya olarak mahkemelerce geçerliliği bulunan pcap dosyalarının incelenmesi ve analizinin yapılması, olayların aydınlatılması aşamasında büyük önem arz etmektedir. Uygulamanın bu aşamasında Wireshark ağ dinleme programı ile yapılan ağ taraması sonucu kaydedilen pcap uzantılı ağ dosyasının NetworkMiner programı ile incelemesi yapılmıştır. Yapılan inceleme sonucu elde edilen veriler Şekil 7 - 10 arasında verilmiştir. Tarama sonucu elde edilen veriler arasında; internet tarayıcı geçmişi bilgileri, kullanıcı adı ve şifre bilgileri, resim ve dosya bilgileri gibi kanıt niteliği taşıyan verilere ulaşılmıştır.

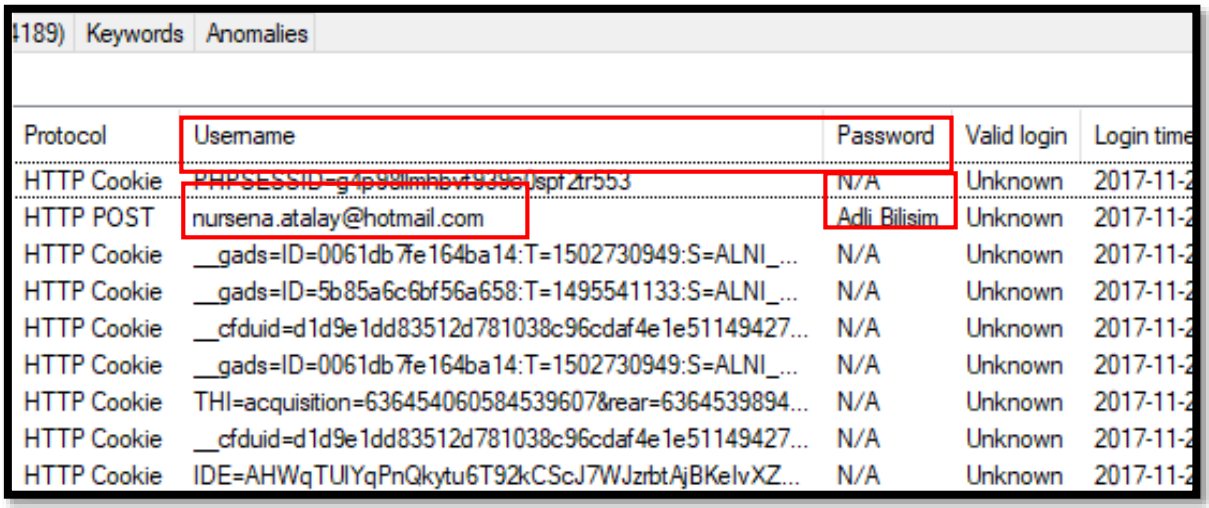


Şekil 7. NetworkMiner ağ analizi programı ile pcap dosyası analizi sonucu internet geçmişi bulguları



Şekil 8. NetworkMiner ağ analizi programı ile pcap dosyası analizi sonucu elde edilen dosya bulguları

Şekil 9. NetworkMiner ağ analizi programı ile pcap dosyası analizi sonucu elde edilen resim dosyası bulguları



Şekil 10. NetworkMiner ağ analizi programı ile pcap dosyası analizi sonucu elde edilen kullanıcı adı ve şifre bulguları

5. Ağ analiz programları yetenek karşılaştırması

Adli bilişim alanında olayların aydınlatılması için inceleme ve analiz aşamasında açık kaynak kodlu veya ücretli olarak birçok inceleme ve analiz programları kullanılmaktadır. Olayların aydınlatılmasında önemli bir rol oynayan ağ analizi için de birçok program kullanılmaktadır. Ağ analizi amacıyla kullanılan bu programlar genel olarak ağ trafiği dinleme, port ve protokol bilgisi öğrenme, paket yakalama ve veri elde etme amacına yönelik olarak hareket etmektedir. Yapılan bu çalışmada, ağ inceleme ve analiz programlarına örnek olarak Nmap, Zenmap ve NetworkMiner programları incelenmiş ve çeşitli uygulamalara yer verilmiştir. Bu bölümde kullanılan bu programların farklı yönlerden yetenek karşılaştırmaları yapılmış ve elde edilen sonuçlar Tablo 5 ile verilmiştir.

Tablo 5. Nmap ve Zenmap ve NetworkMiner programlarının yetenek karşılaştırması [1-6].

YETENEK	Nmap	Zenmap	NetworkMiner
Görsel Arayüz	×	✓	✓
Rapor Çıktısı	✓	✓	✓
Ağ Dinleme	✓	✓	✓
Port Tarama	✓	✓	×
Hızlı Sonuç Bulma	✓	×	×
Ayrıntılı Sonuç bulma	✓	✓	✓
Pcap Uzantılı Dosya İncelemesi	×	×	✓
Windows İşletim Sistemi Desteği	×	×	✓
Linux İşletim Sistemi Desteği	✓	✓	×
Açık Kaynak Kodu	✓	✓	×
Ücretli Yazılım	×	×	✓
Çerez Yakalama	×	×	✓
Paket Kontrolü(Giden-Gelen)	×	×	✓
Hash Hesaplaması	×	×	✓
Port Durum ve Servis Bilgisi	✓	✓	×
Grafiksel Ağ Topolojisi	×	✓	×
Anahtar Kelime Arama	×	×	✓
Kullanıcı Adı ve Şifre Bilgisi	×	×	✓
Dinlenecek Hedef Belirtme	✓	✓	×
Ağ Üzerinde Elde Edilen Resim Dosyaları	×	×	✓
Geçmiş Tarama Bilgisi	×	×	✓
DNS Bilgisi	✓	✓	✓
MAC Adresi Bilgisi	✓	✓	✓
IP Adresi Bilgisi	✓	✓	✓
Ağ Dinleme Zaman Bilgisi	✓	✓	✓

6. Sonuç ve öneriler

Teknolojinin gelişimine bağlı olarak günlük hayatımızın hemen her alanında ağ ve internet kullanımı yaygınlaşmıştır. Bu kullanıma bağlı olarak her geçen gün biraz daha kullanım sayısı arttıkça olumlu yanların yanı sıra olumsuz ve tehlikeli durumları da beraberinde getirmektedir. Bilgisayar korsanları, teknolojiyi ve onu ele geçirme yollarını her geçen gün biraz daha farklı teknikler ile gerçekleştirmektedir. Adli bilişim alanı, dijital ortamlarda gerçekleşen olayların aydınlatılması ve mahkemelerce kanıtların sunulması çalışmalarının bir bütünüdür. Adli bilişim alanında elde edilen kanıt

ve veriler çeşitli ücretli ve ücretsiz programlar ile gerçekleşmektedir. Adli bilişim alanında olayların aydınlatılmasında ve kanıtların elde edilmesinde, günlük hayatımızın hemen her alanında karşımıza çıkan ağ kullanımının analizi büyük rol oynamaktadır. Bu alanda ağ analizinin önemi, bir mahkemede güvenlik saldırılarının kaynağı hakkında kanıtsal bilgi elde etmek amacıyla ağ olaylarının yakalanması, kaydedilmesi ve analizi olarak tanımlanabilmektedir. Adli bilişim alanında ağ analizi, temel olarak ağ trafiğinin analiz edilmesine dayanmaktadır. Analizin gerçekleşmesi için ağ trafik kaydı tutan cihazların ve sistemlerin kayıtlarına ihtiyaç duyulmaktadır. Kayıtların tespiti Nmap ve Zenmap gibi ağ dinleme ve veri elde etme programları ile kayıtların analizi, NetworkMiner, WireShark vb. programları ile geçekleşmektedir.

Bu çalışmada, adli bilişim, ağ güvenliği ve ağ analizi konularına detaylı olarak yer verilmiş ve adli bilişim alanında olayların aydınlatılmasında ağ analizinin kullanımı ve öneminden bahsedilmiştir. Ağ analizin de kullanılan programlardan olan Nmap, Zenmap ve NetworkMiner programları incelenmiş ve programlar ile yapılan çeşitli uygulamalar sonucu elde edilen bulgular görselleştirilerek açıklanmıştır. Son olarak kullanılan ağ analizi ve veri elde etme amacıyla kullanılan bu programlar arası yetenek karşılaştırmaları yapılarak karşılaştırma bulguları tablo ile sunulmuştur.

Kaynaklar

[1] Suarez F.J., Pelayo N. 2015. Modeling and Simulation of Computer Networks and Systems Methodologies and Applications, Edited by Mohammad S. Obaidat, Petros Nicopolitidis, Faouzi Zarai, 187-223, Spain.

[2] Mohan V.P, Anuradha J. 2015. Network Security and Types of Attacks in Network, International Conference on Intelligent Computing, Communication & Convergence, Bhubaneswar, Odisha, India.

[3] Meghanathan N., Allam S.R., Loretta A. 2009. Tools and Technıques for Network Forensics. International Journal of Network Security & Its Applications (IJNSA), 1 (1).

[4] Orebaugh A., Becky P. 2008. Nmap in the Enterprise-Using Zenmap. Edited by Aaron W. Bayles, USA, 137-159.

[5] Orebaugh A., Becky P. 2008. Nmap in the Enterprise-Using Zenmap Edited by Aaron W. Bayles, USA, 87-136.

[6] Pilli E.S., Joshi R.C., Rajdeep N. 2010. A Generic Framework for Network Forensics, International Journal of Computer Applications, 1 (11): 0975 – 8887.