# Yerel Alan Ağları İçin IP Tabanlı Saldırı Tespit Uygulaması ve Güvenlik Önerileri

[1]M.Zekeriya Gündüz, [2]Resul DAŞ

***Abstract* – The increase of the quantity and the value of the information committed via the internet, establishing a connection with the whole world in a very short period of time has attracted the attention of criminals and directed them to the internet. The criminals adapting to this new world quickly developed themselves in the field of technology rapidly, and began to commit crimes, which are normally too difficult to commit in normal ways, through the internet easily. These crimes called as cyber-crimes are intruding or attacking to a system or any informatic device by the person or persons in virtual platform. In this paper study is presented a sample attack was carried out on the local area network. Then the attacker was detected through IP.**

***Index Terms* - Intrusion Detection Systems, Computer Network Security, Cyber Crime, Information Security.**

***Özet*- İnternet üzerinden işlenen bilginin miktarı ve değerinin artması, bütün dünya ile çok kısa bir sürede bağlantı kurulabilmesi, suçluların da ilgisini çekmiş ve internete yönelmelerini sağlamıştır. Bu yeni dünyaya çok hızlı adapte olan suçlular, kendilerini teknoloji alanında da hızlı bir şekilde geliştirmiş, normal yollar ile oldukça zor gerçekleşecek suçları, internet ortamından kolay bir şekilde yapabilmeye başlamışlardır. Bilişim suçları olarak adlandırılan bu suçlar, sanal ortamda kişi veya kişiler tarafından bir sisteme veya herhangi bir bilişim cihazına izinsiz girme veya saldırıda bulunmadır. Bu makale çalışmasında, yerel alan ağı üzerinde bir saldırı gerçekleştirilmesi sunulmaktadır. Daha sonra saldırgan IP tabanlı tespit edilmiştir.**

***Anahtar Kelimeler* - Saldırı Tespit Sistemleri, Bilgisayar Ağ Güvenliği, Siber Suçlar, Bilgi Güvenliği, Bilgisayar Güvenliği.**

## I. GİRİŞ

Teknoloji alanındaki gelişmeler büyük bir ivme kazanarak hızlı bir şekilde değişmekte ve insanların yaşamını kolaylaştıran çok önemli unsurlar haline gelmektedir. Günlük iş süreçlerinin elektronik ortamlara taşınması, manyetik ortamdaki bilgilerin paylaşılması, e-devlet uygulamaları gibi önem arz eden konular yaygınlaşmaktadır. Bu sebeple, kurulan bu sistemlerin bilişim ağ güvenliğinin gerekliliği ve önemi son derece önemlidir. Bu bağlamda olası tehdit ve tehlikelerin araştırılıp, bunlara karşı gerekli önlemlerin alınmasının, bilgi, bilgisayar ve bilgisayar ağ güvenliğinin sağlanması açısından oldukça önem kazandığı görülmektedir. [1]-[3].
Son yıllarda internetin yaygın kullanımının artmasıyla, sanal ortamda oluşabilecek dijital saldırılarda buna paralel olarak artmaktadır. Bu saldırılar, kritik iş uygulamalarında ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmuştur.

[1]Bingöl Üniversitesi, Teknik Bilimler Meslek Yüksek Okulu, Bingöl / TÜRKİYE (tel: 0505-9505544; e-mail: zekeriyagunduz@gmail.com )
[2]Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, Elazığ / TÜRKİYE (e-mail: resuldas@gmail.com)

Bilgisayar virüsleri, DoS saldırıları, şirket çalışanlarının hataları, bilgisayar ağları üzerinde hâlâ büyük bir tehlike oluşturmaktadır. Bununla beraber kurum ve kuruluşlar, sanal dünyanın uçsuz bucaksız ortamında ağ saldırıları ve ağda yapılan aldatmacalara karşı güvenliklerini sağlamak için güvenlik politikaları da uygulamak zorunda kalmaktadırlar [4].

Bu makale çalışmasında, bir yerel alan ağında ARP Poisoning (ARP zehirlemesi) yöntemi ile bir saldırı gerçekleştirilmiş olup, bu saldırının nasıl tespit edilebileceğine yönelik bir uygulama çalışması yapılmıştır. IP tabanlı tespit edilen saldırgan ve belirtilen çözüm önerilerine göre elde edilen bulgular değerlendirilmiş olup sistem kullanıcıları ve son kullanıcılara yönelik ağ güvenliğinin sağlanması açısından alınabilecek güvenlik önlemleri maddeler halinde sunulmuştur.

## II. AĞ GÜVENLİK ARAÇLARI ve SALDIRI YÖNTEMLERİ

Bir ağ sisteminde sistem yöneticilerinin ağı izlemek için kullandıkları ağ izleme yazılımları bazı durumlarda saldırganların elinde tam bir silaha dönüşebilmektedir. Beyaz şapkalı veya etik hacker olarak tanımlanan kişiler genellikle bu araçları, sistemdeki eksiklikleri bulmak için kullanırken, siyah şapkalı veya saldırgan olarak adlandırılan kişiler ise bunları sistemlere zarar vermek ya da veri hırsızlığı için kullanırlar.

Bilgi sistemlerinin güvenliklerini sağlamak amacıyla birçok çalışma yapılmaktadır. Bu çalışmalar genelde sisteme; güvenlik duvarları kurmak, saldırı tespit sistemleri kurmak, güvenli iletişim protokolleri sağlamak, zarar verici kodlara karşı yazılımlar kullanmak gibi çözümler olabilir. Fakat tüm bu yapılan çalışmalardan sonra bile sistemde saldırganların sızabileceği açıklar olabilir. Bu açıklar çeşitli güvenlik araçları kullanılarak tespit edilebilir ve gerekli önlemler alınabilir. Güvenlik araçları ayrıca sistemi izleme olanağı da sunarlar. Var olan güvenlik araçları genelde bilgisayar sistemlerine saldırı amacıyla geliştirilmiştir. Buradaki temel düşünce sistemin açıklarını saldırganlardan önce ortaya çıkarmak ve gerekli önlemleri almaktır [5],[6].

Bu çalışmada, ağı izlemek için kullanılan güvenlik araçları ve saldırı yöntemlerinin genel özellikleri şu şekildedir:

*Cain & Abel*

Ağ yöneticileri, güvenlik uzmanları ve geliştiriciler için üretilmiş, hedef ağda paket analizi yapma, ağdan şifre gibi bilgileri çekme, şifrelenmiş bilgileri Brute Force (kaba kuvvet) ve Cryptanalysis (şifreleme) metotları ile çözme gibi işlevlerinin yanında kötü niyetli kullanılmak istendiğinde tam bir silaha dönüşebilen yazılım aracıdır. ARP Poisoning saldırılarında en iyi sayılabilecek

yazılımlardan biridir. Güvenli protokollerde bile ARP Poisoning yaparak paket analizi yapabilir, şifrelenmiş veriyi okuyabilir. Ayrıca Cain & Abel Microsoft işletim sistemleri için bir password kırma aracı olarak da kullanılabilmektedir. Cain & Abel programının Linux sistemler için kullanılan formatı DSniff programıdır [7].

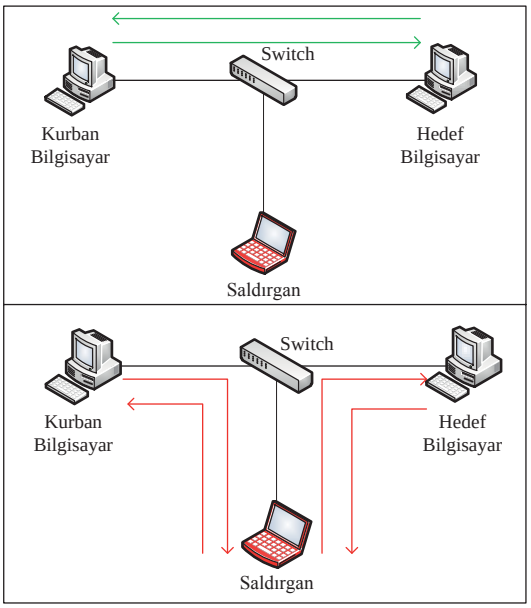
*Wireshark*

UNIX ve Windows platformları için ücretsiz bir ağ protokolü analizcisidir. Canlı bir ağda veya daha önceden diske kaydedilmiş bir ağ verisi üzerinde çalışarak ağ incelemesi yapar. Kullanıcı, interaktif bir şekilde incelenen veri hakkında ayrıntılı bir bilgi alabilir. Bu bilgi tek bir paket için de söz konusudur. Güçlü özellikleri arasında, zengin bir süzme diline sahip olması ve TCP oturumunu birleştirerek analiz imkanı sağlaması vardır. Wireshark programı Ethereal olarak adlandırılan programın yenilenmiş versiyonudur. Wireshark 750 den fazla protokolü analiz etme özelliğine sahiptir. Belirli kriterlere göre filtreleme yapabilmesi de kullanımını kolaylaştırmaktadır. Diğer paket yakalama yazılımlarının dosyalarını da açabilmektedir [8].

İnternet ortamında veya yerel ağ ortamlarında gerçekleştirilen saldırı ve aldatmaca yöntemlerinden bazıları; DoS saldırıları (Smurf saldırıları, Ping Flood saldırıları, SYN Flood saldırıları gibi), Spoofing saldırıları (ICQ Spoofing, DNS Spoofing, IP Spoofing, E-mail Spoofing gibi) bunların yanında SQL Injection, Sniffing, ARP Poisoning, DNS Poisoning ve DNS Cache Poisoning olarak belirtilebilir. İnternet gibi geniş alan ağlarında güvenlik politikaları tam uygulanmış ise bu saldırı türlerinin uygulanabilirliği çok daha zordur. Ancak yerel alan ağlarında bu saldırı yöntemlerinin gerçekleştirilebilirliğinin daha fazla ve kolay olduğunu söylemek mümkündür. Bu çalışmada bir yerel ağda saldırı için ARP poising yöntemi kullanılmıştır.

*ARP Poisoning*

ARP, veri göndermek için IP adresinin MAC adresini çözümlemeye yarayan protokoldür. ARP paketleri taklit edilerek saldırgan kendi makinesine verileri yönlendirebilir. Saldırgan ARP poisoning yaparak iki bilgisayar arasındaki trafiğin ortasına geçebilir. Şekil 1'de üst kısım normal ağ trafik akışını gösterirken, alt kısım ise ARP Poisoning saldırısının bulunduğu durumdaki ağ trafik akışını göstermektedir. Saldırgan, IP adresini ve MAC adresini gateway gibi broadcast yayın yaparak duyurur. Kurbanın ağ trafiği, saldırgan üzerinden geçmeye başlar ve saldırgan, kurbanın ağdaki tüm verilerini takip edebilir [6].

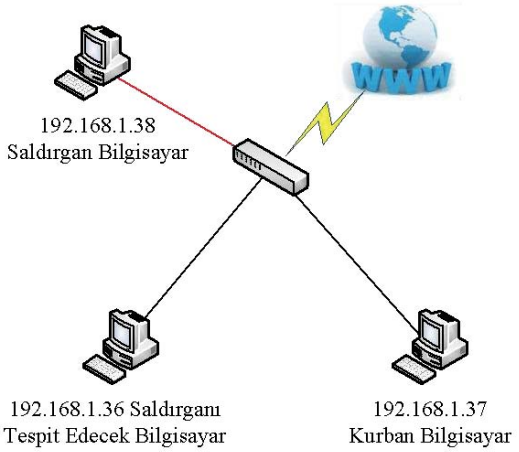



Şekil 1. ARP poisoning saldırı şeması [6]

## III. YEREL ALAN AĞINDA VERİ HIRSIZLIĞI UYGULAMASI

Bu bölümde, yerel bir ağ sisteminde gerekli önlemler alınmadığı takdirde bilgisayarlar üzerinde üçüncü kişiler tarafından sniffing işleminin ne kadar kolay gerçekleştirilebileceğini gösteren uygulamalar yapılmıştır. Ağda, istenilen kullanıcının web üzerinde girdiği siteler, kullanıcı adı, şifre bilgileri ve girdiği sitelerdeki hesaplarının ele geçirilebileceği örnek bir uygulama ile gösterilmektedir.

Kapsamlı olan bu uygulamada, saldırı aşamasında kurban bilgisayarın dinlenmesi ve kurbana dair sniffing işlemi gerçekleştirilirken kullandığı kullanıcı hesaplarının nasıl ele geçirilebileceği gösterilmektedir. Kurban bilgisayarın dinlenmesinin sağlanması için Microsoft işletim sistemleri için bir password kırma aracı olarak da kullanılabilen *Cain & Able* aracı kullanılmıştır. Kurban bilgisayarın saldırgan tarafından dinlenmesi işlemi için, ağ üzerinde *ARP Poisoning* saldırı yöntemi kullanılmıştır. Yapılan saldırının tespiti için *Wireshark* ağ dinleme aracı kullanılmıştır. Wireshark programı aracılığı ile ARP Poisoning saldırısını gerçekleştiren saldırganın, ARP filtrelemesi yapılarak IP numarası üzerinden tespit edilmesi sağlanmıştır. Tespit edilen IP numarasının yerel ağdaki hangi kullanıcıya ait olduğu, bilgisayar adının belirlenmesi ile anlaşılmıştır. Uygulama hem kablolu hem de kablosuz ağlar üzerinde gerçekleştirilmiştir. Şekil 2'de uygulamanın gerçekleştirildiği yerel ağ üzerinde bulunan bilgisayarlar ve görevleri gösterilmektedir.




Şekil 2. Yerel ağ saldırısının genel gösterimi

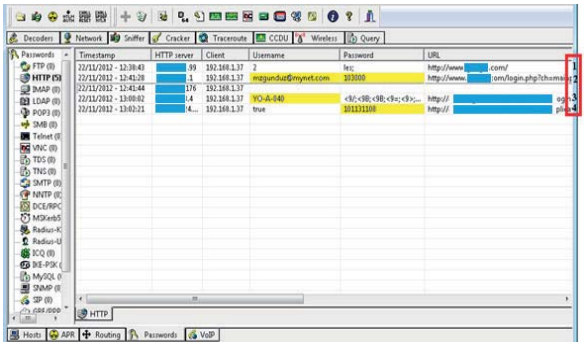
*A. Yerel Ağ Üzerinde Saldırının Yapılması*

Uygulamada kullanılan ARP Poisoning saldırı yönteminin uygulanmasında kullanılan bilgisayarlar ve çalışmamıza yönelik özellikleri şu şekildedir:
192.168.1.38 IP numarası sahibi olan bilgisayar ARP Poisoning saldırısını gerçekleştirecek, üzerinde Cain & Able programı yüklü olan, saldırgana ait bilgisayardır.
192.168.1.37 IP numarası sahibi olan bilgisayar, ARP Poisoning saldırısına maruz kalan, kurban bilgisayardır.
192.168.1.36 IP numarası sahibi olan bilgisayar, ağdaki saldırganı tespit edecek, üzerinde, protokol temelli ağ dinleme yazılımı olan wireshark bulunan bilgisayardır.

Uygulamada bazı portallar ve siteler üzerinde *kullanıcı adı* ve *şifrenin* elde edilmesine yönelik dört farklı sonuç alınmıştır. Bu sonuçlar şu şekilde belirtilebilir:
1) Kullanıcı adı ve şifrenin tespit edilemediği durumlar.
2) Kullanıcı adı ve şifrenin tespit edildiği durumlar.
3) Kullanıcı adının tespit edilip, şifrenin tespit edilemediği durumlar.
4) Kullanıcı adının tespit edilemeyip, şifrenin tespit edildiği durumlar.

Yapılan uygulamada yukarıda belirtilen sonuçlara göre Şekil 3'de gösterilen durumlar elde edilmiştir. Bunlar;
1. sonuçta hesaba dair bilgiler alınamamıştır.
2. sonuçta portaldan kullanıcı adı ve şifre bilgileri elde edilmiştir.
3. sonuçta kullanıcı adı elde edilmiş olup, password şifreli olarak iletildiğinden ağ üzerinden elde edilememiştir.
4. sonuçta kullanıcı adı elde edilememiş, password elde edilmiştir. Username alanı boolean bir değer döndürmektedir. Bu değerin SQL Injection yöntemleri ile atlatılarak sisteme girilebileceği düşünülmektedir.

Şekil 3 üzerindeki sonuçlar, gerçek uygulama sonuçları olduğu için bazı veriler kurum ve kuruluşların itibarını zedelememek adına gösterilmemiştir.

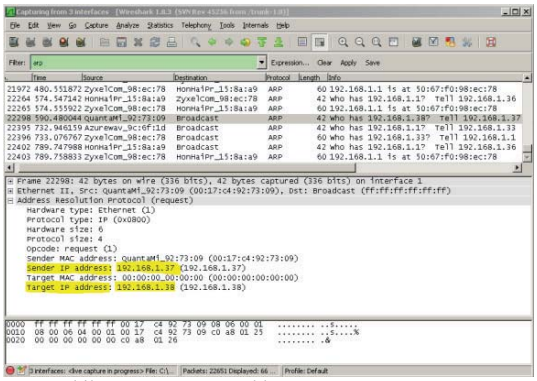


Şekil 3. Saldırı aşamasının sonuçları

*B. Saldırganın Ağ Üzerindeki IP Adresinin Tespiti*

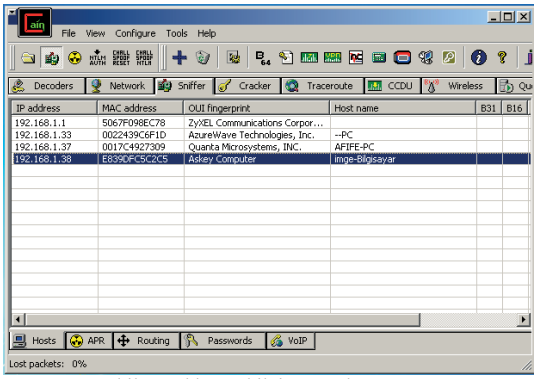
Saldırı hazırlık ve saldırı aşamalarından sonra saldırganın ele geçirdiği bilgiler, saldırgan tarafından kullanılabilecektir. En azından saldırgan istediği tüm bilgilere ulaşamasa bile yerel ağda elde ettiği bilgilerden yola çıkarak istediği kullanıcı üzerinde çeşitli sosyal mühendislik aldatmacaları ile istediği bilgilerin tamamına yakınını elde edebilecektir.

Bu çalışmada, *ortadaki adam* (Man in the Middle) saldırılarından olan ARP Poisoning saldırısının tespiti wireshark programı ile ARP filtresi üzerinden veri paketlerinin incelenmesi ile gerçekleştirilmiştir. Buna göre Şekil 4'de saldırı anında elde edilen wireshark çıktısı incelendiğinde; geçit yolunun (gateway) tüm bağlantı noktaları ile temas halinde olduğu görülmektedir. Ancak, saldırgan IP sinin kurban IP si ile de temas halinde olduğu tespit edilmiştir. Bu ilişkinin detayları incelendiğinde ise Şekil 4'ün alt kısmında görüldüğü gibi kurbanın verilerinin saldırganın IP adresine yönlendirilmiş olduğu gözlemlenmiştir.



Şekil 4. Wireshark ile saldırganın IP adresinin tespiti

Şekil 5'de saldırganın yerel ağda tespit edilen IP numarasının ağdaki başka bir bilgisayardan, Cain & Able programı kullanılarak bilgisayar adı ve MAC adresi tespit edilmiştir. Saldırganın bilgisayarının adı "imge-Bilgisayar" olduğu görülmektedir. Aynı şekilde kurban bilgisayarın IP adresi incelendiğinde bilgisayar adının "AFIFE-PC" olduğu görülmektedir.




Şekil 5. Saldırgan bilgisayar adının tespiti

### C. Uygulama Sonuçları

Uygulama basamaklarındaki sonuçlar çizim modellemeleri ile gösterilmek yerine gerçek çıktıları ile gösterilmiştir. Buradaki amaç, hiçbir kurum ya da kuruluşun itibarını zedelemek değil, farkındalık oluşturma amaçlı ağ saldırılarının varlığını göstermektir. Ayrıca bu uygulamalar ile paylaşıldıkça artan bir nesne olarak da tanımlanan bilginin, korunumu ve güvenliği için alınacak tedbirlerin belirlenmesinde katkıda bulunmak amaçlanmıştır. Unutulmamalıdır ki, bir saldırının nereden ve ne şekilde geleceğini bilmek en iyi savunma sanatıdır. Uygulama sonucunda elde edilen bulgulara göre aşağıda belirtilen önemli çıkarımlar elde edilmiştir:

1) Farklı yerel alan ağlarında yapılan uygulamalarda, kablosuz yayın yapan erişim noktalarının (access point) güvenliklerinin genellikle doğru yapılandırılmadığı tespit edilmiştir. Eğer gerekli güvenlik önlemleri alınmadı ise; basit bazı işlemler ile bu erişim noktalarının ağlarına dâhil olunarak istenilen kullanıcılar izlenebilmekte, hatta yönetim paneli ele geçirilebilmektedir.
2) HTTPS protokolünü kullanan sitelerden veri çalınması http ve diğer protokolleri kullanan sitelere göre daha zordur.
3) Wireshark gibi ağ paketleri üzerinde her türlü analizi yapabilen programlar kötü niyetli kullanıcılar elinde bir silaha dönüşebilir. Bu duruma; ağda MSN programı üzerinden görüşme yapan kullanıcıların konuşma metinlerinin ele geçirilmesi örnek olarak gösterilebilir.
4) Kriptolamalı şifrelerin kırılması neredeyse imkânsızdır. Teorik olarak kırılması mümkün olsa bile, uygulamada kriptolu şifrenin elde edilmesi uzun süre ve yüksek maliyet gerektireceğinden dolayı mümkün değildir.
5) Cain & Able aracı ile yapılan uygulamalarda güvenilirliğe önem veren sitelerden ilk denemede bilgiler çalınabildiği halde sonraki denemelerde başarılı olunamamıştır. Kurum ve kişilerin itibarını zedelememek açısından ekran çıktıları verilmemiştir.
6) Saldırının varlığını tespit eden bazı sitelerin Şekil 6'da görüldüğü gibi sunucularına erişimi engelledikleri tespit edilmiştir.


Şekil 6. Güvenlik sertifikası

7) Bazı sitelerin Şekil 7'de görüldüğü gibi kullanıcı adı ve şifre istenecek formlarında hemen *https* protokolüne geçtikleri görülmektedir.


Şekil 7. HTTPS protokolü

## IV. SONUÇ VE ÖNERİLER

Bilişim teknolojilerinin yaygınlaşması ile günlük hayatımızdaki iş ve işlemler elektronik ortamlarda artık daha hızlı yapılmaktadır. Bu durum, bilgi güvenliğinin sağlanmasını zorunlu hale getirmektedir. Bu nedenle kullanıcılar yaptıkları iş ve işlemlerde bilginin öneminin farkında olup, bu konuda güvenlik unsurlarını, politikalarını ve güvenlik süreçlerini uygulamak zorundadırlar. Böylece belli oranda, karşılaşılabilecek sorunlar ve tehlikeler azaltılabilecek, işgücü, zaman ve parasal kayıplar önlenebilecektir. Aynı zamanda, internet üzerinden gelebilecek zararlı yazılımlara veya program parçacıklarına karşı kişisel ve kurumsal bilgi güvenliğinin arttırılmasına katkılar sağlanacaktır.

Bilgi güvenliği konusunda güvenlik açıklarının önlenebilmesi için kişilerin ve kurumların basitten en karmaşık güvenlik yöntemlerine kadar bir dizi önlemler alması gerekir. Ancak, tüm önlemler alınmış olsa da, sürekli geliştirilen saldırı teknikleri yüzünden, hiç kimse ve hiç bir kuruluş kendini %100 güvende hissetmemelidir. Saldırılar; kötü niyetli kişiler, arkadaşlarımız veya tanıdığımız kişilerden gelebilir.

Bu çalışmada kapsamlı literatür taraması sonucunda bilişim suçlarının tespitine yönelik yapılan çalışmalar incelenerek, bilgisayar ağ sistemlerinde yapılan saldırıların, IP tabanlı delil tespitinin yapılması konusunda uygulamalar yapılarak, elde edilen sonuçlara göre; son kullanıcıları ve sistem yöneticilerini yakından ilgilendiren eksiklikler ve alınabilecek önlemler hakkında değerlendirmeler yapılmıştır. Yapılan uygulama aşamalarının ve sonuçlarının değerlendirilmesi neticesinde, ağ sistemlerinde var olan server, switch, hub gibi ağ cihazlarının ve bilgisayarların güvenliğinin artırılmasının yanında, sistem yöneticileri ve son kullanıcılar için aşağıda verilen önemli çıkarımlar belirlenmiştir.

Bilgi güvenliğinin sağlanması adına sistem veya ağ yöneticilerinin alabileceği önlemlerin bir kısmı şu şekilde belirtilebilir:

1) Ağ sistemi üzerinde bulunan güvenlik duvarı üzerindeki yönetim ve güvenlik politikaları analiz edilerek, detaylıca belirlenmelidir.
2) Sunucu hizmetlerinin kullandığı portlar dışındaki diğer kullanılmayan portlar kapatılmalıdır.
3) Ağ trafiğini kontrol etmek ve düzeltmek için VLAN yapıları oluşturulmalıdır.
4) Ağ sisteminde sniffing işlemlerinin tespiti için wireshark gibi birçok ağ dinleme araçları kullanılabilir.
5) Ağ sisteminde yazılımsal veya donanımsal olarak firewall kullanılmalıdır.
6) Saldırı davranışlarının takibi ve analizi için log kayıtları tutulmalıdır. Ayrıca güvenlik duvarlarında log analiz ve yönetim sistemi kullanılmalıdır.
7) Ağda olası tehlikeleri saptamak için IDS/IPS gibi otomatik açık tarama araçları kullanılmalıdır.
8) Ağ ve bilgi güvenliği ile ilgili güncel konular ve bilgiler, özellikle ağ yöneticileri tarafından yakından takip edilmelidir.
9) Dağıtıcı kullanılan sistemlerde güvenliğin sağlanması adına switch veya akıllı switch gibi cihazlar kullanılmalıdır.
10) Sistem için güvenlik politikaları oluşturarak bunların uygulanmasının ve takibinin yapılması sağlanmalıdır.
11) Bazı anahtarlar ve yönlendiriciler üzerindeki yönetim yetkilendirmelerine dikkat edilmelidir.
12) Router ve firewall gibi ağ aktif cihazları üzerinde erişim kısıtlamaları (access-list) oluşturulmalıdır.
13) Sunucu, router, firewall, switch gibi tüm ağ cihazları üzerinde güvenlik önlemleri en başından uzmanlarca yapılıp, herhangi bir güvenlik açığına meydan verilmemelidir.
14) VLAN ağında kullanıcıların yerinin tespit edilmesi için IP temelli erişim kontrol listesi tekniği (IP adresinin erişim yapabileceği portun kenar switch üzerinde sabitlenmesi) kullanılmalı veya her MAC adresinin belli zaman aralığında hangi IP adresini kullandığının kayıt altında tutulmasının en kesin yöntemi olarak yönlendiricinin ARP tablosunun loglanması sağlanmalıdır.
15) Yönlendiricilerin erişim hakları, erişim protokolleri güvenliği, şifrelerin güvenliğinin sağlanması, gereksiz servislerin kapatılması gibi yapılandırma ayarlamaları yapılmalıdır.

Ağ sisteminde ağ yöneticilerinin yanısıra özellikle son kullanıcılar şu hususlara dikkat etmelidir:

1) Web ortamında şahsi bilgiler ve şifre türü veriler dikkatli kullanılmalıdır.
2) Sohbet ortamlarında saldırıların daha fazla olabileceği unutulmamalıdır.
3) Web ortamında güvenliğin hiçbir zaman tam olarak sağlanamayacağı unutulmamalıdır.
4) Güvenilir ve tanınır siteler haricindeki sitelerden dosyalar indirilmemelidir.
5) Bilinmedik ve güvenilirliği şüphe uyandıran sitelere kişisel bilgiler verilmemelidir.
6) Sosyal mühendislik yöntemleri incelendiğinden saldırıların insanın yakınındaki kişilerden de gelebileceği unutulmamalıdır.
7) Kullanıcı internet ortamında kendini %100 güvende hissetmemelidir.
8) İnternet ortamı, gerçek dünyanın, sanal âleme bir yansımasıdır. Bu yüzden sosyal paylaşım sitelerinde paylaşılacak bilgiler dikkatli seçilmelidir.
9) Sazan avlama türündeki saldırılarda çoğunlukla insanların bilgisizliğinden, tecrübesizliğinden ve zaaflarından yararlanıldığı unutulmamalıdır [10].
10) Kişisel, önemli parolalar düzenli bir şekilde değiştirilmelidir.
11) İşletim sistemlerine ait güncellemeler düzenli olarak yapılmalıdır.
12) Lisanslı yazılımlar kullanılmalıdır.
13) Yasal ve güvenli olmayan sitelerden dosya indirme işlemi yapılmamalıdır.
14) İnternet kafe gibi halka açık ve güvenilirliği şüpheli olan ortamlarda internet bankacılık ve e-ticaret işlemleri yapılmamalıdır. Yapılacak ise güvenlik esaslarına dikkat edilmelidir.
15) Online alışverişlerde sanal kredi kartları kullanılmalı ve alışveriş süresince limitleri tanımlanmalıdır.
16) Şüpheli görülen e-posta eklentileri okunmadan ve açılmadan silinmelidir.

Bu çalışmada yapılan uygulamalar sonucunda dünyada ve ülkemizde bilgi güvenliğine yönelik en önemli tehditlerden olan kötücül ve casus yazılımların, yaygın olarak kullanımda olduğu, fakat kullanıcıların bu tür saldırı ve tehditlerden çoğunlukla haberdar olmadığı anlaşılmıştır. Herhangi bir zararla karşılaşılmaması için, konuya gereken önemin verilmesi, bilgi birikiminin arttırılması, bilgi güvenliğine yönelik hassasiyet gösterilmesi ve gereken önlemlerin alınması ile farkındalık oluşturulması gerekmektedir [11].

Bu çalışmanın konu ile alakalı olarak temel kavramsal bilgilerden ziyade uygulamaya yönelik yapılabilecek çalışmalar ve son kullanıcılar ile ağ yöneticilerinin alması gereken önlemler konusunda daha gerçekçi fikirler oluşturabileceği düşünülmektedir. Ayrıca, bu çalışmanın akademik literatüre IP numaralarından yararlanılarak veri hırsızlığının tespit edilmesi konusunda gerçekci bir uygulama ile yeni çalışmalar oluşturulması adına katkıda bulunduğu düşünülmektedir.

## KAYNAKLAR

[1] Y.Uzunay, "Dijital Delil Araştırma Süreci", 2.Polis Bilişim Sempozyumu, Ankara, 2005.
[2] Canbek, G., Sağıroğlu, Ş., "Bilgi, Bilgi Güvenliği Ve Süreçleri Üzerine Bir İnceleme", Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, 06570 Maltepe, Ankara.
[3] Daş, R., Kara, Ş., Gündüz, M.Z., "Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri", 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (5th International Conference on Information Security and Cryptology), 17-18 Mayıs 2012, ODTÜ, Ankara.
[4] Karaarslan E., Teke A., Şengonca H., 2003. Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması, İletişim Günleri, İzmir.
[5] Anuk, E., Güvenlik Araçları, İTÜ Bilişim Enstitüsü, İstanbul.
[6] Gündüz, M.Z., 2013. Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti, Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ.
[7] *Internet:* http://www.oxid.it/cain.html, 21.05.2013.

[8] *Internet:* http://www.wireshark.org/, 21.05.2013.
[9] Elbahadır, H., 2011. Hacking Interface, Kodlab Yayıncılık, İstanbul.
[10] Şenol, A., Karacan, H., "Sazan Avlama (Phishing): Kullanılan Teknikler ve Bunlardan Korunma Yöntemleri" 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (5th International Conference on Information Security and Cryptology), 17-18 Mayıs 2012, ODTÜ, Ankara.
[11] Karadoğan, İ., Daş, R., Baykara, M., "Scapy ile Ağ Paket Manipülasyonu", 1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu), 20-21 Mayıs 2013, Elazığ, Turkey.

**M. Zekeriya GÜNDÜZ,** 1983 yılında Bakırköy'de doğdu. 2006 yılında Süleyman Demirel Üniversitesi, Teknik Eğitim Fakültesi, Elektronik ve Bilgisayar Sistemleri Öğretmenliği bölümünü bitirdi. 2006-2010 yılları arasında Milli Eğitim Bakanlığına bağlı Endüsri Meslek Liselerinde Bilişim Teknolojileri öğretmeni olarak görev yaptı. Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik ve Bilgisayar Eğitimi Anabilim dalında Ağ güvenliği konusunda " Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti" adlı yüksek lisans çalışmasını tamamladı. Halen Bingöl Üniversitesi Teknik Bilimler Meslek Yüksek Okulu, Bilgisayar Programcılığı bölümünde öğretim görevlisi olarak çalışmaktadır.

**Resul DAŞ,** 1975 yılında Elazığ'da doğdu. 1999 yılında Fırat Üniversitesi, Teknik Eğitim Fakültesi, Bilgisayar Öğr. bölümünü, 2002 yılında Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Sistemleri alanında yüksek lisansını tamamladı. 2008 yılında aynı üniversitenin Elektrik-Elektronik Mühendisliği bölümünde doktora eğitimini tamamlayarak, bu alanda Doktor ünvanını aldı. 2000–2011 yılları arasında Fırat Üniversitesi Enformatik bölümünde öğretim elemanı olarak çalıştı. Kasım 2011 yılından beri Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği bölümünde öğretim üyesi olarak görev yapmaktadır. Bilgisayar Ağları, Ağ Güvenliği, Web ve Veri Madenciliği, Bilgi Keşfi, Adli Bilişim ve Güvenlik araştırma konularında çalışmalar yapmaktadır.