LINUX TABANLI SUNUCULARDA VE KABLOSUZ AĞLARDA SİBER SALDIRILARIN TESPİTİ VE ÖNLENMESİ

Samet ZENGİN[1], Erdal IRMAK[2] ve Halil İbrahim BÜLBÜL[3]
[1]Hoca Ahmet Yesevi Üniversitesi, Türkiye Türkçesi ile Uzaktan Eğitim Programları (TÜRTEP), Ankara
[2]Gazi Üniversitesi, Teknoloji Fakültesi, Elektrik Elektronik Mühendisliği Bölümü, Ankara
[3]Gazi Üniversitesi BÖTE / Hoca Ahmet Yesevi Üniversitesi, TÜRTEP, Ankara
samet_zengin@yahoo.com; erdal@gazi.edu.tr; bhalil@gazi.edu.tr

ÖZET

Bu çalışmada, kablosuz ağlarda gerçekleştirilen şifre kırma saldırılarının ve Linux tabanlı sunucu sistemlerine yönelik önemli bir tehdit olan SSH kaba kuvvet saldırılarının, oluşturulan uygulama ortamlarında deneysel olarak test ve analizi gerçekleştirilmiştir. Ayrıca SSH kaba kuvvet saldırılarının, ELK-SIEM sistemi ile gerçek zamanlı ve ilişkisel tespit analizleri ve raporlama süreci üzerinde durulmuştur. Saldırı tespit ve önleme işlemleri metodolojik olarak ele alınmış ve analiz için gerekli veriler adım adım toplanarak yorumlanmıştır. Saldırıların hangi açıklıkları daha etkili kullanabildiği, gerçekleşme sürecinde izlenen yöntemler ve saldırının sonuçları, bütüncül bir yaklaşımla ve örnek deneysel uygulamalarla aktarılmıştır. Elde edilen sonuçlar ışığında, saldırılara karşı alınması gereken önleme teknikleri ve karşı aksiyonlar önerilmiştir. Çalışmanın, gün geçtikçe önemi artan kurumsal ve bireysel bilgi güvenliğinin sağlanmasına katkı sağlayacağı düşünülmektedir.

Anahtar Kelimeler- Kaba Kuvvet Saldırısı, SIEM Sistemleri, Syslog Filtreleme, Kablosuz Ağ Saldırıları

DETECTION AND PREVENTION OF CYBER ATTACKS ON WIRELESS NETWORKS AND LINUX BASED SERVERS

ABSTRACT

In this study, experimental testing and analysis of password cracking attacks on wireless networks and SSH brute-force attacks on Linux based server systems are carried out through sample application test environments created for the study. Furthermore, real time and relational detection and reporting analysis of SSH brute force attacks by using the ELK-SIEM system is emphasized. Intrusion detection and prevention processes are handled methodologically and the data required for analysis are collected systematically. Weaknesses that attacks can use more effectively, methods followed during the realization of attacks and their results are given through a holistic approach and sample experimental applications. Considering the results obtained, prevention techniques and counter-actions to be taken against the attacks are proposed. It is believed that the study will contribute to maintaining institutional and individual information security, the importance of which increases day by day.

Keywords- Brute Force Attack, SIEM Systems, Syslog Filtering, Wireless Network Attacks

I. GİRİŞ (INTRODUCTION)

Günümüzde gelişen saldırı teknikleri nedeniyle Linux sistemlerin savunması büyük önem arz etmeye başlamıştır. Temel bilgisayar bilgisine sahip kişiler bile internette çeşitli fiyatlarda satılan araçları kullanarak yüksek bilgi birikimi ve beceri isteyen saldırıları gerçekleştirebilmektedir. Bu tarz uygulamaların bir pazarı olması nedeniyle her geçen gün daha da gelişmekte ve sistemlerin yeni zafiyetleri tespit edilip bu saldırı araçları güncellenmektedir. Hal böyle iken Linux sunucu sistemlerine yapılan saldırıların tehdit riski daha da artmıştır. Siber saldırganların öncelikli hedefi bilgi sistemini ele geçirmektir. Bu açıdan akla gelen ilk saldırı kaba kuvvet (brute force) saldırılarıdır. Bu saldırıların Linux sistemlere yönelik yapılanına SSH kaba kuvvet saldırısı da denmektedir. Sistem parola ile korunuyorsa kaba kuvvet saldırısıyla şifrenin kırılması gereklidir. Bu amaç için daha önceden hazırlanmış sayılar, harfler ve özel karakterler bulunan bir "*Pass List*" hazırlanır. Şifreye ulaşmak için denemeler yapılır ve doğru şifreyi bulana kadar devam edilir [1, 2]. Şifre tespitine yönelik gerçekleştirilen bir saldırı olmasına rağmen artçı etkileri ile servis reddine sebebiyet vermektedir. Yeteri kadar güvenli bir şifre

kullanılmaması halinde yüksek başarı oranlarına sahiptir.

Kaba kuvvet saldırıları da dâhil olmak üzere siber tehditlerin tespiti ve önlenmesinin önemi gün geçtikçe artmakta ve literatürde önemli çalışmalar sunulmaktadır.

- [3] no.lu çalışmada, mahrem bilgilerin savunması için saldırı tespit sistemlerinin vazgeçilmez hale geldiği ifade edilmiştir.
- [2]'de, bal küpü sistemleri ile saldırı tespit ve önleme sistemleri arasında karşılaştırmalar yapılmış ve daha yüksek koruma güvenliği gerekli olan ortamlar için Bal küpü sistemleri önerilmiştir. Hatta daha önce hiçbir şekilde bilinemeyen sıfırıncı gün açıklıklarına karşı dahi yüksek etkileşimli dinamik bal küpü sistemler ile savunma ve tespit çalışmaları yapılabileceği vurgulanmaktadır.
- [4]'te, geleneksel saldırı tespit sistemlerinin eksikleri ve buna karşı yeni bir yapay zekâ destekli tespit sistemi yaklaşımı anlatılmaktadır. Yapay zekâ destekli denetimin kontrol edilen sistemdeki olağan dışı hareketlerin etkilerini takip ederek gelişen saldırı tekniklerine karşı daha isabetli kararlar alınması amaçlanmıştır.
- [5]'te, web sunucu günlük (log) kayıtlarını inceleyerek saldırı izlerini ve anomali hareketlerini kontrol etme mantığı üzerine kurulmuş bir saldırı tespit sistemi sunulmaktadır.
- [1]'de, kaba kuvvet saldırılarının tespiti ve önlenmesi için örnek bir olay incelenmiş ve saldırıya uğramış bir bilgisayarın *Syslog* verileri incelenerek saldırı izlerinin tespit edilebileceği ifade edilmiştir. Günlük kayıtları silinmiş bir geçmiş saldırının tespiti için ise *FTK Imager* programı ile disk imajları alınarak ve *Access Data Forensic Toolkit* programı kullanılarak saldırı izleri tespit edilmiştir.

Linux sistemlerinde, SIEM yazılımları anlık saldırı tespiti ve saldırı raporları oluşturarak sistem yöneticisine tehdit istihbaratı sağlayabilmektedir. Ayrıca dağıtık halde olan kayıtları bir yerde toplayarak ve oluşturulan mantıksal kuralları kullanarak gerçek zamanlı korelasyon yapılabilir ve normalde tespit edilemeyen güvenlik olayları tespit edilebilir [6]. SSH kaba kuvvet saldırılarının tespiti her ne kadar kod betikleri ile yapılabilse de bu tespit eksik kalmaktadır. Dolayısıyla SIEM sistemleri ile ilişkisel ve anlık tehdit istihbaratı sağlayan bir sistem kullanılmalıdır.

Siber güvenliğin bir diğer önemli boyutu, kablosuz ağlardan gelen saldırılardır. Günümüzde kablolu internet ağlarının kullanımı oldukça düşmüştür. Kablosuz ağlar ise yapısı gereği bazı güvenlik açıklıkları barındırmaktadır. Saldırganlar, bu açıklıkları kullanarak ağdaki veri paketlerinden bilgileri çalabilmektedirler. Radyo dalgaları yayan erişim noktası, kablosuz ağa dâhil olan kullanıcılara veri paketlerini iletmektedir ama ağa dâhil olmayan bilgisayarlar da bu paketlere erişebilmektedir [7]. Bu duruma karşı şifreleme algoritmaları geliştirilmiştir. Fakat gelişen saldırı teknikleri ile eski algoritmalar güvensiz hale gelmiştir. Güncel şifreleme teknikleri olan *WPA2* ya da *WPA+TKIP* (*Temporal Key Integrity Protocol*) kullanılması tavsiye edilmekle birlikte bunların kimlik doğrulama saldırılarına karşı açık teşkil ettiği de göz önünde bulundurulmalıdır [8]. Bu dezavantaj kimlik doğrulama konusunda kablosuz ağlara hizmet aksatma saldırısı yapılabilmesine yol açmaktadır. Saldırıların önlenememesinde en önemli unsur, farklı cihazlardan saldırı gelmesi ve MAC adreslerinin tespit edilmesindeki zorluktur. Adeta bir hayalet cihazdan saldırı gelmesi durumu gibi bir sorun ortaya çıkmaktadır. Bu nedenle saldırılar, klasik önleme yöntemleri çoğu zaman yetersiz kalmaktadır. Ağ güvenliğini tehdit eden unsurların artmasıyla birlikte anti virüs ve güvenlik duvarı gibi sistemler uzun süre güvenlik sağlayamamaktadır [7].

Yukarıdaki duruma örnek olarak [9] no.lu çalışmada, kablosuz yerel ağlara yönelik kaba kuvvet yöntemi ile şifre kırma denemeleri yapılmış ve kısa ya da bilinen şifrelerin hemen kırılabileceği ortaya çıkarılmıştır. Saldırıları gerçekleştiren cihazın tespiti yapılamadığı için kablosuz ağ erişim noktasının görünürlüğünün gizlenmesi şeklinde çözüm tavsiye edilmiştir. [10]'da, kablosuz ağlara yapılan saldırılarda en sık görülenlerden birinin DoS (*denial-of-service*) saldırıları olduğu belirtilmiş ve günümüzde bu saldırılara karşı güvenlik zafiyeti giderilmiş routerler üretilse de bunun başka zafiyetlere neden olduğu ortaya konulmuştur. Ele alınan örnek olayda, sistemi aksattırma ve performansını düşürme derecesinde etkili saldırılar yapılabildiği gösterilmiştir. [8]'de, *WEP* ve *WPA-TKIP* gibi şifreleme algoritmalarına sahip olmayan routerler için TCP/Syn Taşması Saldırısı, UDP Taşması Saldırısı, Ping Taşması Saldırısı türlerinin önemli tehditler oluşturduğu ortaya konulmuştur. Ayrıca bahsedilen koruma protokollerini kullanan kablosuz ağlarında 802.11 Associate/Authenticate Taşması Saldırısı, 802.11 Beacon Taşması Saldırısı, 802.11 Deauthenticate Taşması Saldırısı karşısında korumasız olduğu ifade edilmektedir

[11] nolu çalışmada, kablosuz ağ güvenliğinde yapılan saldırıların tespit edilmesinin oldukça güç olduğu ve bunun için ağ üzerindeki bir bilgisayardan ağ trafiğinin analiz edilmesi gerektiği belirtmektedir. [12]'de, kablosuz ağa dâhil olan bir saldırganın HTTP üzerinden akmakta olan internet trafiğindeki verileri elde etmesinin mümkün olduğu ifade edilmektedir. Her ne kadar HTTPS protokolü bu saldırılara karşı korusa da web uygulamalarının kullandıkları API sistemlerinde yeterli güvenlik tedbirleri olmayabileceği fark edilmiştir. [13]'te, *Scapy* ile kablosuz ağda paket manipülasyonu incelemesi yapılmaktadır. Bu aracın, ağ üzerindeki birçok paketi yakalayabildiği, istenmeyen

kaynaklara paket trafiklerini kesebildiği ya da değiştirebildiği, *WEP* şifrelemesi kullanan güvenli ağda paket içeriklerini görüntüleyebildiği ancak gerçek zamanlı çalışmalarda yavaş kaldığı ve daha fazla hafıza kullanımına sebep olduğu belirtilmektedir. [14]'te, *IPSec* özelliğinin IPv4'te isteğe bağlı olmakla birlikte IPv6 da zorunlu olduğu, ortak bir işleyiş içinde oldukları için güvenlik açığı oluştuğu, bu durumun kablosuz ağ trafiğinde veri gizliliğini riske attığı ve verilerin dinleme saldırısına karşı açık hale geldiği belirtilmektedir.

Yukarıda özetle verilen bilgi ve gereksinimlerden dolayı bu çalışmada kablosuz ağlara yapılan saldırılar, Linux tabanlı sunucu sistemlerine yapılan SSH kaba kuvvet saldırıları ve anlık saldırı tespit raporları oluşturma sürecinde yaşanan problemler ele alınmıştır. Literatürde benzer çalışmalar bulunmaktadır. Fakat bunların büyük bir kısmının teorik çalışmalar olduğu görülmüştür. Bu makalede ise bahsedilen saldırıların tespiti ve önleme yöntemleri uygulamalı olarak test edilmiştir. Elde edilen sonuçlar ve bulgular doğrultusunda yorumlar yapılmış ve bazı kritik önerilerde bulunulmuştur.

II. DENEYSEL YÖNTEM VE TEST ORTAMI (EXPERIMENTAL METHOD AND TEST PLATFORM)

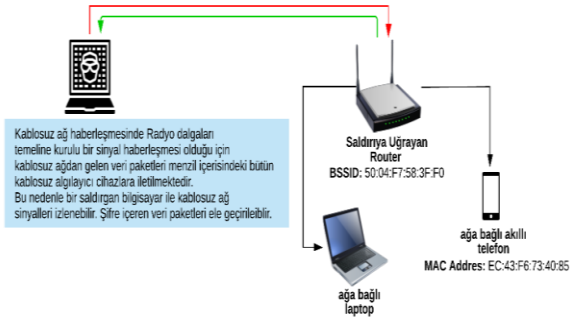
Çalışma üç ana konuya yoğunlaşmıştır. Bunlar; kablosuz ağlara yapılan şifre kırma saldırıları, Linux tabanlı sunucu sistemlerinde SSH kaba kuvvet saldırıları ve Linux tabanlı sunucularda SSH kaba kuvvet saldırılarının SIEM programları ile tespit edilmesi ve saldırı raporları oluşturmaya ilişkin süreç şeklindedir.

2.1 Kablosuz Ağ Saldırısı

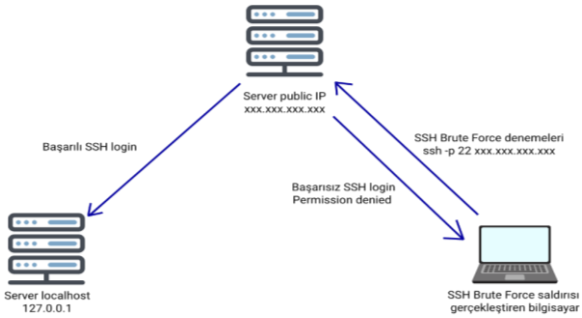
Bu bölümde, kablosuz ağlara yapılan şifre kırma saldırısı gerçek bir router üzerinde gerçekleştirilerek saldırının hangi şartlarda başarıya ulaşacağı veya ulaşamayacağının analizi yapılmıştır. Test ortamı Şekil 1'de verilmiştir. Kablosuz ağ erişim noktası olarak *TP Link MR6400/ 4G Router*, saldırgan bilgisayarı olarak Linux tabanlı *Ubuntu 20.04* işletim sistemli bir dizüstü bilgisayar, ağa bağlı bilgisayar olarak *Windows 10 Pro* işletim sistemli bir masaüstü bilgisayar ve ağa bağlı akıllı telefon olarak *Android 10* işletim sistemli bir cep telefonu kullanılmıştır. Saldırı senaryosuna göre Linux işletim sisteminden kablosuz ağa şifre kırma saldırısı için *Aircrack-ng* aracı kullanılmaktadır. Bu araç ile ağ trafiğindeki veri paketleri dinlenerek yakalanmakta ve bunlar içerisinde şifre taşıyan paket aranmaktadır. Bu amaçla, *Aircrack-ng* aracındaki kabiliyetler sayesinde bir şifre havuzu kullanılarak *sözlük atağı* olarak bilinen saldırı tekniği gerçekleştirilmektedir. Paket yakalandığında '*handshake'* uyarısı verilmektedir. Ağ şifreleri genellikle *WPA-WPA2* algoritmaları ile şifrelenmiş ağ paketleri içerisindedir. Dolayısıyla saldırgan, ağdan yakalanan ve şifre bilgilerini içeren veri paketlerini, şifre havuzunda bulunan ön tanımlı şifrelerle eşleştirmek için tersine mühendislik yürütmektedir.

2.2 Linux Tabanlı Sunucularda SSH Kaba Kuvvet Saldırısı

Bu senaryoda, *syslog* verilerinin analizi yapılarak saldırı tespiti yapılmaktadır. Ağ tabanlı bir sunucuya saldırı denemesi yapmak yasal olmadığından bu çalışmada bireysel kullanımdaki gerçek bir adanmış (*dedicated*) sunucuya SSH kaba kuvvet saldırısı gerçekleştirilmektedir. Adanmış bir sunucu kullanılması, sistem kaynaklarının başka kullanıcılarla paylaşılmadığını ifade etmektedir. Saldırı test düzeneği Şekil 2'de verilmiştir.



Şekil 1. Kablosuz ağ saldırısı için test ortamı



Şekil 2. SSH kaba kuvvet (brute force) saldırı ortamı

2.3 ELK-SIEM ile Gerçek Zamanlı Raporlama

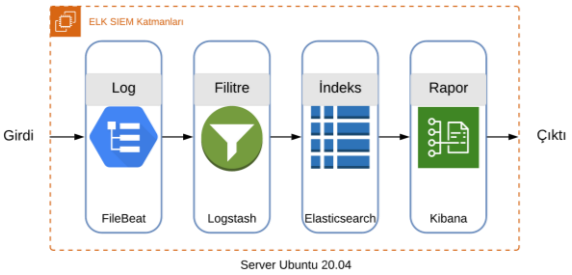
Bu çalışmada, saldırı tespit ve uyarı sistemi olarak ELK-SIEM tercih edilmiştir. SIEM sistemleri, sunucudan gelen bütün günlükleri (log) toplayan, filtreden geçirip dizin (indeks) kaydı alan ve elde ettiği dizin bilgileri ile oluşturduğu tehdit istihbaratları üzerinden alarm bildirimi üreten siber güvenlik sistemleridir. Görsel yönetim paneli ile kolay kullanım sunması, işlevsel kullanım alanlarının çok olması ve sistem kaynağı kullanımı ihtiyacının düşük olması nedeniyle tercih sebebi olmuştur. Bu sistem ile *Ubuntu 20.04* işletim sisteminin *syslog* verileri analiz edilerek SIEM raporları oluşturulmaktadır. Sistemin işleyişi Şekil 3'te verilmiştir.

Bu işleyişe göre Ubuntu sunucuya SSH kaba kuvvet saldırısı gerçekleşir. Bu saldırı */var/log/auth.log* dosyasında sistem tarafından bütün oturum açma (login) denemeleri ile birlikte kayıt altına alınır.

'*Filebeat*', işletim sisteminde tutulan günlükleri (log) alır ve filtrelerden geçirilmek üzere '*logstash*' tarafına iletir. Filtre edilmiş veriler '*Elasticsearch*' tarafına iletilir ve dizin (indeks) kaydı alınarak kullanıma hazır hale getirilir. *Kibana*, dizinlenmiş verileri kullanarak ve görselleştirerek raporlama ve yönetim paneli olarak çalışır.

III. DENEYSEL ÇALIŞMALAR (EXPERIMENTAL STUDIES)

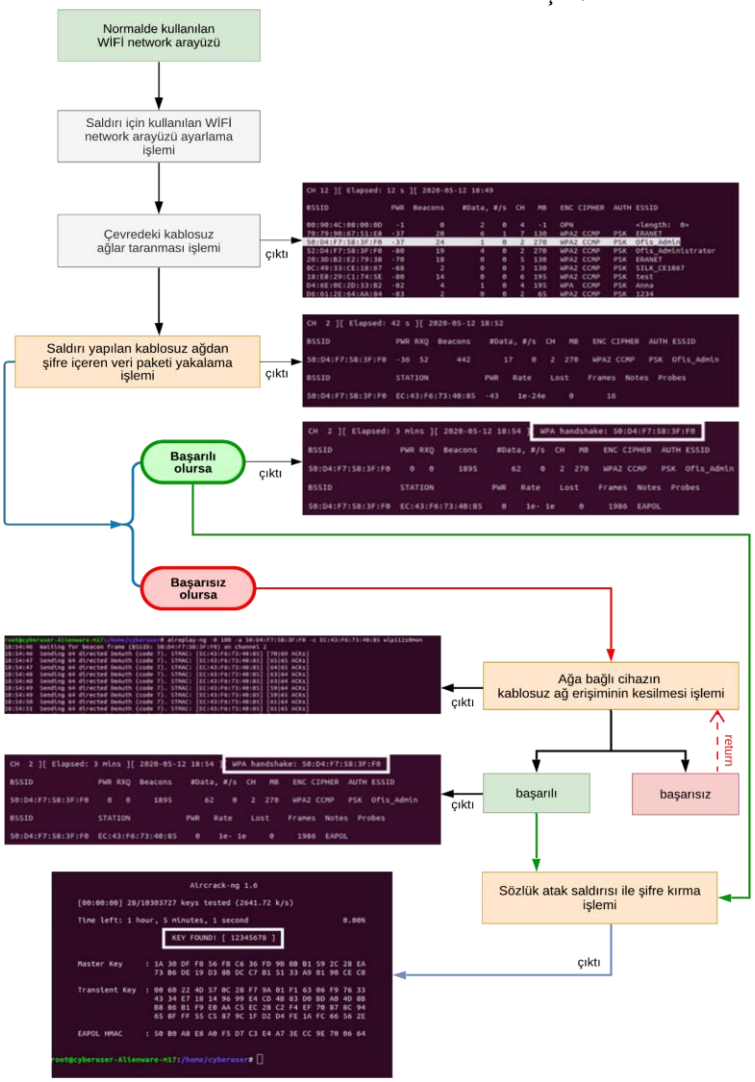
Bu bölümde, yürütülen deneysel çalışma adımları ve test prosedürü ayrıntılı olarak verilmiştir. Saldırıların gerçekleştirilmesi ve tespit edilmesi işlemleri ayrı başlıklarda ele alınmıştır. Elde edilen gözlem ve bulguların yorumlanması ise bir sonraki bölümde verilmektedir.



Şekil 3. ELK-SIEM işleyiş şeması

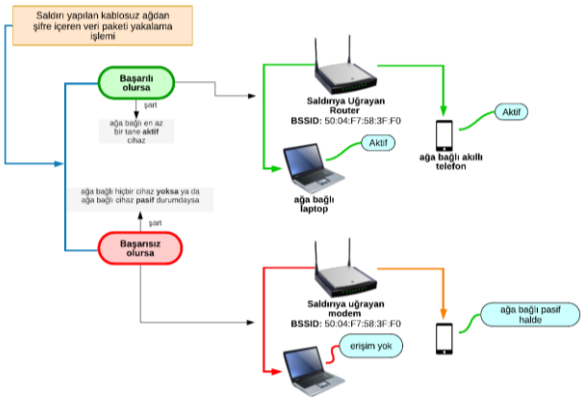
3.1 Kablosuz Ağ Saldırısı (Wireless Network Attack)

Gerçekleştirilen saldırı senaryosunda, saldırganın başarıya ulaşması için gerekli olan iki durum mevcuttur. Birinci aşama, saldırı başlangıcından itibaren başlayıp şifrenin başarılı bir şekilde elde edilebildiği ana kadar olan işlemleri içerir. İkinci aşama ise, ilk aşamada izlenen tekniklerle şifrenin elde edilememesi durumunda başlayan ve alternatif bir teknik uygulanarak şifrenin elde edildiği ana kadar olan süreci içerir. Bütün bu aşamalar ve gerçekleştirilen saldırıların olay akış şeması, Şekil 4'te blok diyagramı olarak verilmiştir.



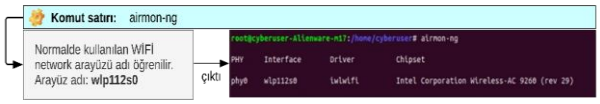
Şekil 4. Kablosuz ağ saldırısı akış şeması

Gerçekleştirilen saldırının başarılı veya başarısız olacağı koşullar, Şekil 5'te gösterilmektedir.



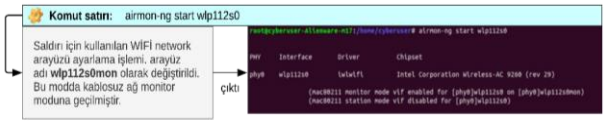
Şekil 5. Saldırının başarılı veya başarısız olacağı koşullar

İlk olarak başarılı saldırı durumu incelenecektir. Saldırı işlemi için öncelikle '*ifconfig*' ya da '*aircrack-ng*' komutu ile kablosuz ağa bağlı bulunulan ara yüz isimi kontrol edilmektedir. Daha sonra buradaki ara yüz ismi kullanılacaktır (Şekil 6).



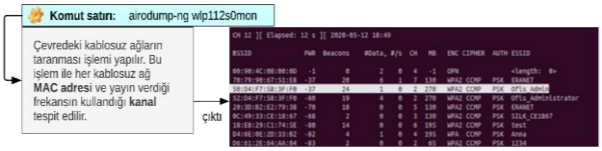
Şekil 6. Kablosuz ağ algılayıcı ismini öğrenme

Kablosuz ağa bağlı bulunulan ara yüz adı (*wlp112s0*) kullanılarak, *wlp112s0mon* isminde saldırı için sahte bir ara yüz ismi oluşturulmaktadır (Şekil 7).



Şekil 7. Kablosuz ağ algılayıcı ismini değiştirme

Sahte internet ara yüzü oluşturulduktan sonra çevredeki bütün kablosuz ağlar taranarak MAC adresleri ve kablosuz ağdaki sinyal aldığı kanal bilgileri listelenmektedir (Şekil 8).



Şekil 8. Ağ üzerinde MAC adresinin tespiti

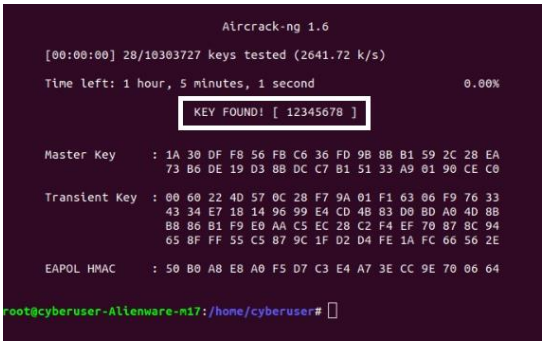
Şekil 8'de görünen *Ofis_admin*, saldırı yapılacak ağdır. Bu çıktıda elde edilen verilerden MAC adresi ve kablosuz ağ kanal numarası (*CH*) sonraki işlemde kullanılacaktır. *airodum-ng* komutu ile belirtilen MAC adresine sahip kablosuz ağın şifre bilgilerini taşıyan veri paketi yakalanmaya çalışılmaktadır. Bu komut çalıştırıldığında Şekil 9'daki gibi bir çıktı alınmaktadır. Burada *BSSID*, saldırı yapılan routerin MAC adresidir. *STATION* kısmında yazan MAC adresi de o ağa bağlı olan her hangi bir cihazın MAC adresidir. Kurban olarak seçilen ağa bağlı cihazlar internette trafik oluşturdukça saldırı uygulaması paketleri yakalayabilecektir. Bu şekilde şifre bilgisi bulunan paket yakalandığında kullanıcıya '*handshake'* şeklinde bir bildirim verilmektedir. Paketin yakalandığı an Şekil 10'da gösterilmektedir.

Şekil 9. Şifre içeren paketleri yakalama işlemi

Şekil 10. Şifre içeren ağ paketinin yakalandığı an

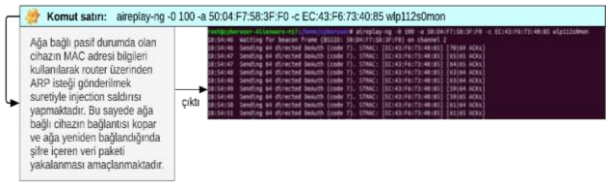
Şifreli paket yakalandıktan sonra içerisindeki gizlenmiş şifre tersine mühendislik tekniği ile kırılmaktadır. Bu amaçla, yakalanan ağ paketi sözlük atak saldırısına tabi tutulmaktadır. Şekil 11'deki komut çalıştırılarak şifre havuzundaki (*rockyou.txt*) bütün şifreler denenmektedir. Şekil 12'te görüleceği üzere, şifre başarıyla bulunmuştur.

Şekil 11. Ağ paketinin şifresini çözme işlemi



Şekil 12. Ağ şifresinin tespit edilmesi

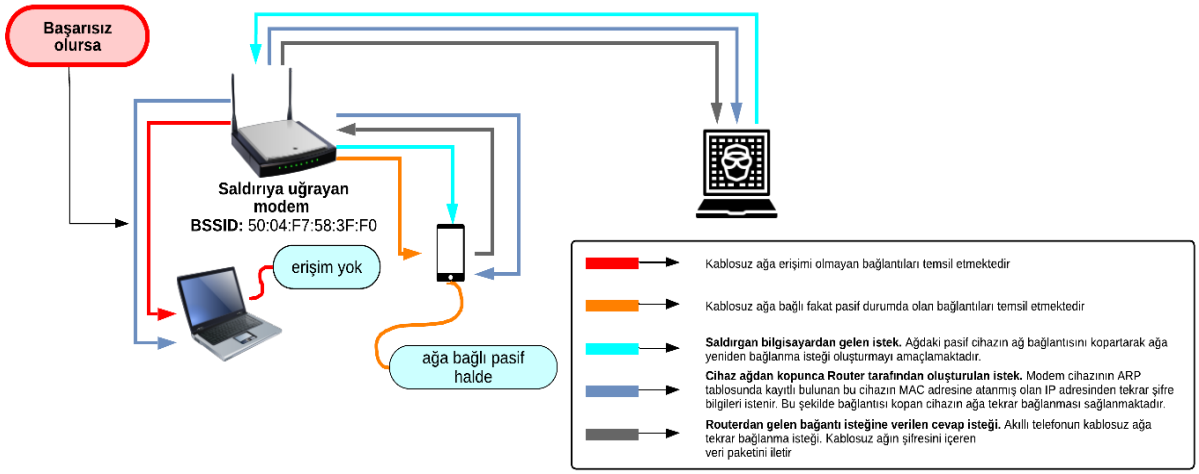
Şekil 5'te gösterilen birinci durumun detayları yukarıda akış şemaları ile detaylıca verilmiştir. Bundan sonraki aşamada Şekil 5'deki ikinci durum olan, ilk denenen saldırı tekniklerinin başarısız olması nedeniyle alternatif saldırı tekniklerinin uygulanması üzerinde durulacaktır. Birinci durumda denen saldırı tekniğinin başarısızlığının sebebi aslında ağa bağlı cihazların pasif durumda olmasıdır. Bu nedenle şifre içeren veri paketi elde edilememektedir. Bu durumu aşabilmek için saldırgan, kablosuz ağ ile ağa bağlı cihazın bağlantısını koparark cihazın ağa yeniden bağlanmasını sağlamaya çalışmaktadır (Şekil 13).



Şekil 13. Ağa bağlı cihazın bağlantısının kopartılması

Kablosuz ağ bağlantısı kopan cihaz, istek göndererek şifre bilgilerini sormak suretiyle ağa yeniden bağlanmaya çalışır. Kablosuz ağlar ve cihazlar bağlantı kurma işlemlerinde ARP istekleri kullanırlar. Ağa bağlı her cihaza DHCP tarafından manuel olarak atanmış IP adresleri ARP tablosunda kayıtlı tutulur. Bu şekilde kablosuz ağ ile cihazın bağlantısı kesildiğinde, bu tablodaki MAC adresine atanmış olan IP adresine ağa yeniden bağlanma isteği gönderilir. Aslında kablosuz ağ yapısı gereği bu istek bütün cihazlara ulaşmaktadır. Fakat sadece belirli bir MAC adresine hitap ettiği için diğer cihazların bağlantısında bir aksamaya neden olmamaktadır. Saldırgan bilgisayardan ise bağlantısı kesilmek istenen cihazın MAC adresi hedef alınmak suretiyle benzer şekilde ARP doğrulama istekleri gönderilmektedir. Sonuç olarak ağa bağlı pasif durumda bekleyen cihazın mevcut ağ bağlantısının kopması sağlanmaktadır. Bu durum yüksek şifreleme güvenliği sağlamak için geliştirilmiş WPA-WPA2 algoritmalarının, yapısı gereği beraberinde getirdiği zayıflıklarıdır.

Burada anlatılmış olan olaylarla ilgili işleyiş, Şekil 14'te sunulmaktadır.



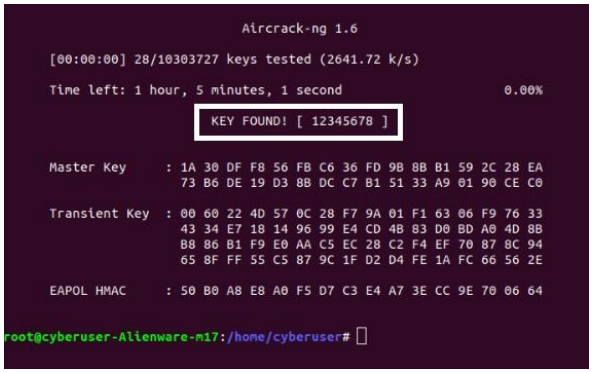
Şekil 14. Saldırgan bilgisayarın kullanmış olduğu protokol ve ağ istekleri

Kablosuz ağ cihazına gönderilen şifre içeren veri paketlerinin radyo sinyalleri menzil içerisindeki bütün cihazlara iletilmektedir. Monitör modunda kablosuz ağ ve kurban cihazın trafiklerini izleyen saldırgan zaten kendisine ulaşan sinyalleri sniffing teknikleriyle rahatlıkla elde etmektedir.

Sonuç olarak kablosuz ağ cihazından tekrar bağlanma isteği alan cihaz kablosuz ağın istemiş olduğu ağ şifre bilgisini içeren veri paketlerini TCP protokolü ile iletmektedir. Şifre bilgisi doğru olduğunda TCP-ACK yani TCP el sıkışma olayı gerçekleşmektedir. Bu şekilde ağdan kopan cihaz ağa tekrar bağlanırken saldırgan da ekranında 'handshake' yani el sıkışma bildirimi almaktadır (Şekil 15 ve Şekil 16).

Ele geçirilen ve şifre bilgilerini içeren WPA-WPA2 algoritmaları ile kriptolu TCP veri paketi, yine kaba kuvvet saldırı teknikleri ile çözümlenmektedir. Veri paketleri, önceden tanımlanmış sık kullanılan şifreler ve bazı karakter kombinasyonları ile ve tersine mühendislik teknikleri kullanılmak suretiyle WPA-WPA2 algoritması ile önce kriptolu hale getirilmektedir. Daha sonra çalınmış ve aynı algoritma ile şifrelenmiş olan kriptolu şifre ile eşleştirme denemeleri yapılmaktadır. Bu saldırının adına sözlük atak saldırısı da denmektedir.

Şekil 15. Ağa bağlana cihazdan şifre içeren TCP veri paketinin elde edilmesi



Şekil 16. Kablosuz ağ şifresinin tespit edilmesi

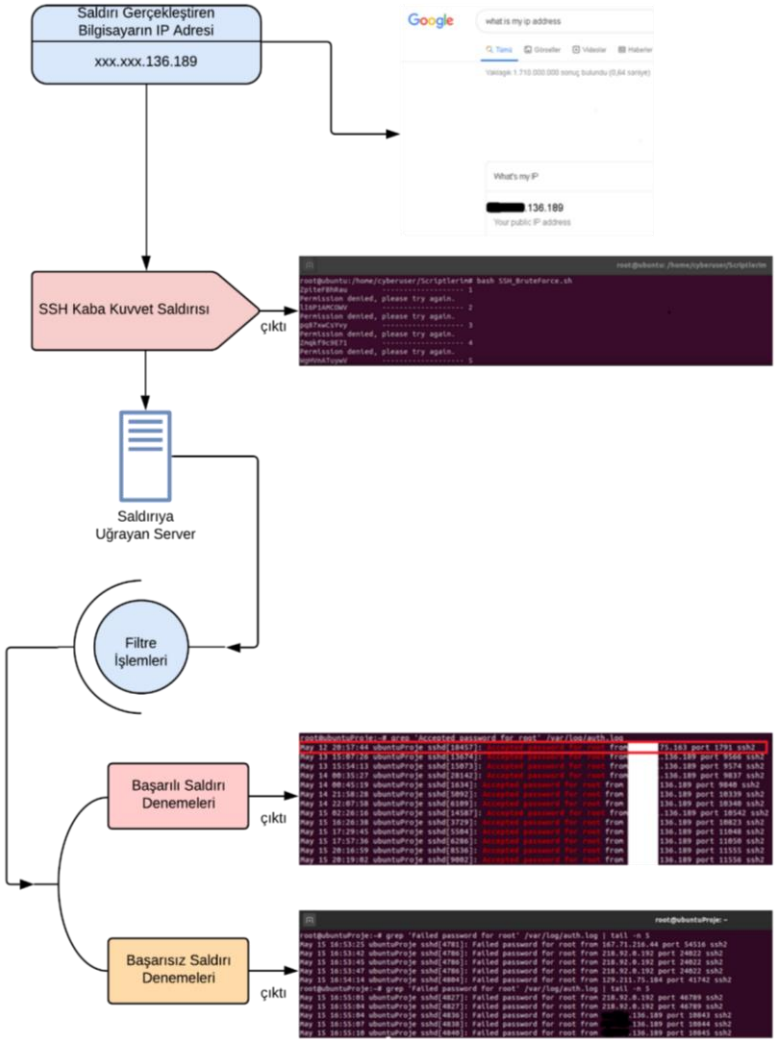
Başarıya ulaşma süresi bilgisayarın işlemci gücü ile ters orantılıdır. İşlemci gücü arttıkça şifre tespiti için geçen süre kısalmaktadır.

3.2 Linux Tabanlı Sunucuya Yapılan SSH Kaba Kuvvet Saldırısı

SSH kaba kuvvet saldırısı, makale yazarlarının kişisel kullanımında olan gerçek bir sunucuya gerçekleştirilmiş ve veriler toplanmıştır. Esasen temel SSH oturum açma (login) denemeleri yaparak şifreyi kırmaya çalışmak maksadıyla gerçekleştirilen bir saldırıdır. Bu saldırılarla zayıf, tahmin edilmesi kolay ya da bilinen klasik şifrelerin kırılması oldukça kolay olduğu görülmüştür.

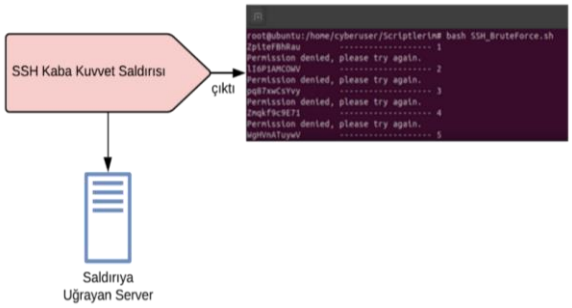
SSH kaba kuvvet saldırılarının izlemiş olduğu prosedürler, akış şeması olarak Şekil 17'de gösterilmektedir.

Kaba kuvvet saldırısına basit bir kod betiği ile başlanmıştır. Bu illegal bir betik olmayıp *ssh -p 22 root@xxx.xxx.xxx.xxx* gibi sunucu yöneticilerinin her zaman kullanmış olduğu bir komuttur. Bu komut tekrar tekrar denenerek her defasında şifre havuzundan başka bir şifre test edilmek suretiyle saldırı gerçekleştirilir.



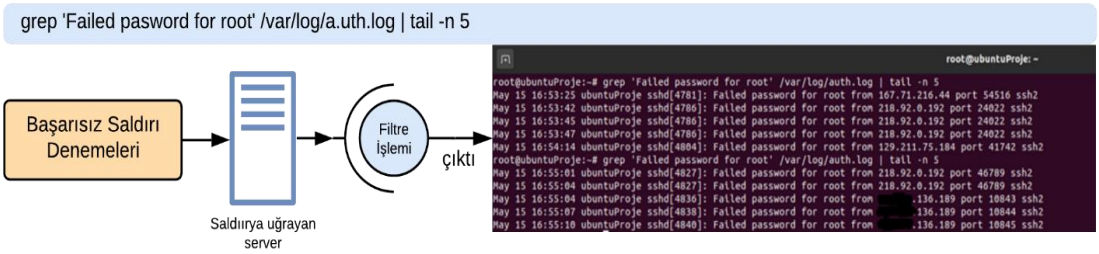
Şekil 17. Linux sunucuya SSH kaba kuvvet saldırısı

Saldırı verileri ve *syslog* dosyaları */var/log* dosyası içerisinde normal verilerle karışık depolanmaktadır. SSH giriş kayıtları bu günlük (log) dosyasına kayıt edilir. */var/log/auth.log syslog* dosyaları içerisinden *grep 'Accepted password for' /var/log/auth.log* komutu ile başarılı SSH oturum başlatma girişleri ve *grep 'Failed password for' /var/log/auth.log* komutu ile başarısız SSH oturum başlatma denemeleri tespit edilebilir. Saldırı öncesinde, saldırı gerçekleştirecek bilgisayarda arama motorunda '*what is my ip*' sorgusu yapılarak kendi IP adresimiz xxx.xxx.136.189 olarak tespit edilmiştir. Bunun amacı saldırı sonrası bu IP'den gelen istekleri, saldırı yapılan sunucu bilgisayardan tespit etmek ve böylece saldırının amacına uygun çalıştığını göstermektedir. Şekil 18'de saldırının gerçekleştirilme anı görünmektedir. Saldırı, rastgele şifreler üreterek SSH oturum başlatma denemeleri yapan ve *Linux Shell* dilinde yazılmış olan '*SSH_BruteForce.sh*' dosyası ile yapılmaktadır.

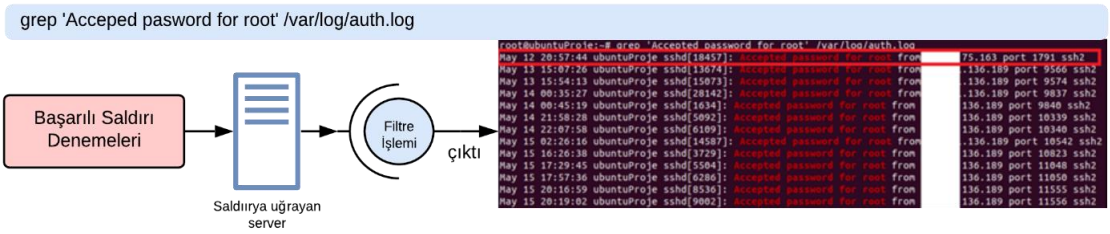


Şekil 18. Sunucuya yapılan SSH kaba kuvvet saldırısı

Şekil 19'da, *grep 'Failed password for root' /var/log/auth.log | tail -n 5* komutu kullanılarak son gerçekleşen 5 saldırı listelenmiştir. Saldırı başlamadan önce belirtilen IP'den saldırı geldiği tespit edilmiştir. Ayrıca başarısız SSH giriş kayıtlarının yanı sıra başarılı SSH giriş günlükleri de filtrelenmelidir. Daha öncesinde sunucuda başarılı oturum başlatan bir saldırı gerçekleşmiş olabilir. Bununla ilgili günlük kayıtları ise *grep 'Accepted password for root' /var/log/auth.log* komutu kullanılarak filtre edilmektedir. Şekil 20'de, başarılı girişler verilmiştir. Bu şekilde, mevcut IP adresi dışında başka bir ağdan da sunucuya başarılı SSH girişi yapıldığı tespit edilmiştir. Bu bilinmeyen oturum açma işlemi teknik olarak başarılı saldırı gibi görünse de söz konusu IP yine aynı ortamdaki ikinci routere olduğu için gerçekte başarılı bir saldırı değildir. Sonuç olarak kaba kuvvet saldırısına ait veriler başarılı şekilde elde edilmiştir.



Şekil 19. Başarısız saldırı tespit işlemi

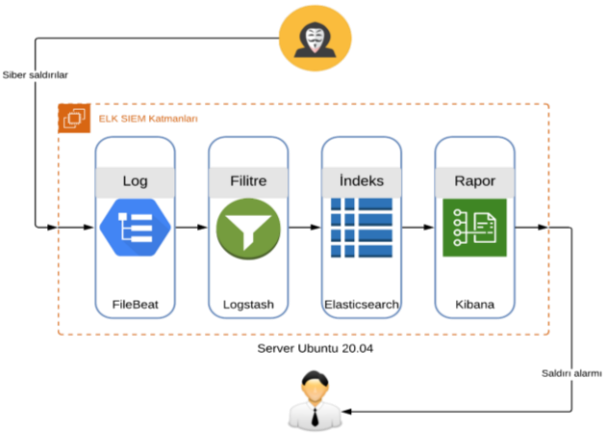


Şekil 20. Başarılı saldırıların tespiti

3.3 ELK-SIEM Sisteminde SSH Kaba Kuvvet Saldırısı

SIEM sisteminde verilerin toplanması işlemi, öncelikle VMware sanal bilgisayar ortamında *Ubuntu 20.04* işletim sistemi üzerine kurulu olan ELK-SIEM yazılımı üzerinde yürütülmüştür. Dolayısıyla ilk saldırı testleri, yazarların kişisel kullanımına ait bilgisayarda, sanal ortamda kurulu bir yerel sunucuda gerçekleşmektedir. Daha sonra gerekli ön test ve denemeler yapıldıktan sonra işlemler gerçek sunucu ortamında sürdürülmüştür.

Saldırı verilerinin rapor haline getirilmiş şekilde toplanması amaçlanmaktadır. SSH raporlarını görüntülemek için *Kibana* kontrol panelinden *Dashboard* bölümüne geçilip *'[Filebeat System] SSH login attempts ECS*' yazan alana giriş yapılmalıdır. Şekil 22'de görüleceği üzere, bu işlem sonrasında ekranda *syslog*, *sudo commands* ve *SSH login* gibi bölümler çıkmaktadır. *Syslog* kategorisinde, işletim sisteminin temel günlükleri (log) ile ilgili veri raporları bulunmaktadır. *Sudo commands* bölümünde işletim sisteminde çalıştırılan tüm betik komutları ile ilgili raporlar tutulmaktadır. *SSH logins* bölümünde ise SSH oturum açma olayları ile ilgili verilerin raporları bulunmaktadır.



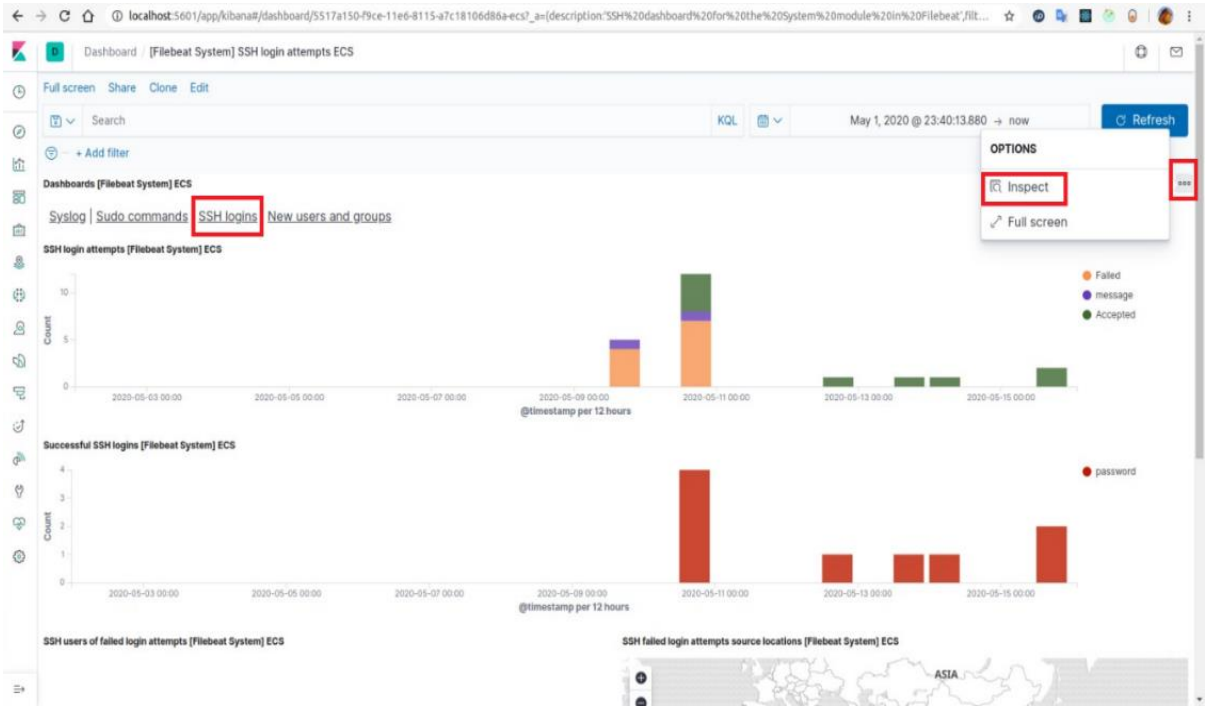
Şekil 21. ELK-SIEM sistemi çalışma mekanizması

Şekil 22. ELK-SIEM ile SSH giriş denemelerinin raporlanması

Şekil 23'de, gerçekleşmiş olan SSH oturum başlatma (login) olaylarının verileri görülmektedir. Açık turuncu renkteki veriler başarısız olayları, yeşil renkteki veriler başarılı olayları, mor renkteki veriler peş peşe üç kez yanlış girilmiş bir oturum açma işleminin ret mesajını, koyu turuncu renkteki veriler ise başarılı oturum işlemlerinde hangi metot kullanıldığını raporlar. Bu çalışmada *password* metodu kullanılmıştır. Burada *password* etiketi oturum açma işleminde yetki doğrulamada kullanılan tekniği ifade etmektedir.

Örneğin eğer *DSA*, *RSA* ve *ECDSA* gibi algoritmalar kullanarak giriş yapılırsa, oturum başlatma yöntemi *SSH Key* tekniği denebilirdi.

Rapor verilerinin çıktısı alınmak istendiğinde, *'inspect'* seçeneği üzerinden rapor alınabilir. Böylece, ELK-SIEM sisteminde toplanan kaba kuvvet saldırı verileri, istenen dosya formatı seçilerek indirilebilir.



Şekil 23. ELK-SIEM olay raporları alanı

IV. DENEYSEL SONUÇLAR (EXPERIMENTAL RESULTS)

Önceki bölümde metodolojik bir yaklaşımla gerçekleştirilme süreci verilen saldırıların detaylı olarak yorumlanması ve elde edilen bulguların her bir saldırı için değerlendirilmesi bu bölümde yapılmıştır.

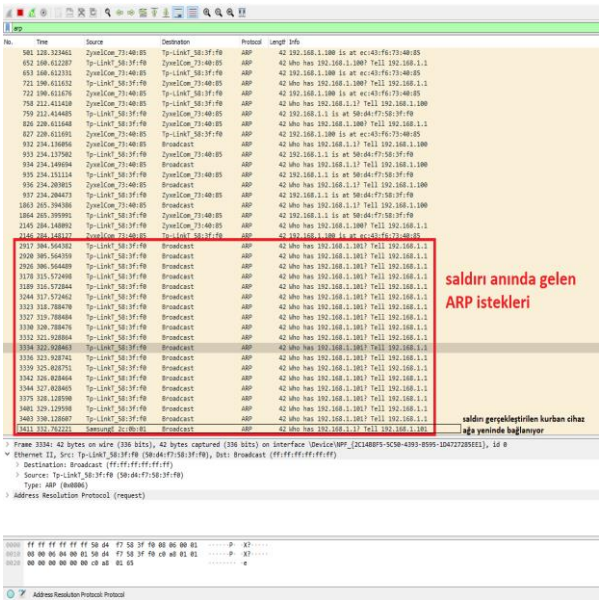
4.1 Kablosuz Ağ Saldırısı

Yapılan çalışmada saldırıyı gerçekleştiren bilgisayar kablosuz ağ dışındadır. Saldırının yapılacağı ağa bağlı bilgisayarda ise *Wireshark* programı ile ağdaki ARP isteği oluşturan paket trafiği incelenmiştir. Saldırı başladığında ağa bir anda çok miktarda ARP istekleri gelmeye başladığı saptanmıştır. Fakat saldırı isteği gönderen cihazın MAC adresi bilgisi ya da cihaz model ismi gibi bir bilgiye ulaşılamamaktadır.

İncelenen ARP isteklerinin kaynağının kablosuz ağ cihazı olduğu tespit edilmiştir. Saldırıya uğrayan kurban cihaz, ağ erişiminin kopartılması sebebiyle DHCP tarafından atanmış mevcut IP adresi üzerinden ağa tekrar bağlanma isteği göndermektedir. Fakat kurban cihaz saldırıya uğradığı için bir türlü kablosuz ağa bağlanamamaktadır. Saldırı devam ettiği sürece kurban cihaz kablosuz ağa her bağlanmak istediğinde bağlantısı kopartıldığı için bu ARP istekleri tekrar etmektedir. Kurban cihaz yeniden bağladığında şifre bilgilerini içeren veri paketlerini kablosuz ağ cihazına tekrar göndereceği için saldırgan bu bilgileri içeren paketi elde etmektedir. Bu olayla ilgili ARP isteklerini gösteren bir ekran görüntüsü Şekil 24'de verilmiştir.

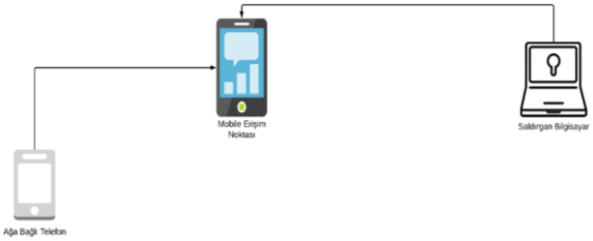
Saldırı anında ağa çok sayıda ARP isteği geliyor olması daha detaylı incelenmiştir. Bu süreçte öncelikle ağa bağlı bir cihaz bulunmadığında saldırı gerçekleştirilmiştir ve saldırgan bilgisayarın şifre içeren ağ paketini yakalayamadığı tespit edilmiştir. Aynı saldırı işlemi ağa bağlı aktif bir cihaz varken gerçekleştirildiğinde saldırı yapan bilgisayar ağ paketini yakalayabilmiştir. Bulgular ve ARP istekleri incelendiğinde, saldırgan ağa bağlı aktif cihazların MAC adreslerini tespit edebilirken kendisini fark ettirecek herhangi ARP isteği oluşturmadığı bulgusuna ulaşılmaktadır.

Bazı durumlarda ağa bağlı bir cihaz tespit edilebilse bile saldırgan şifre içeren veri paketini yakalayamamaktadır. Bu durumda saldırı yapan bilgisayar *aireplay-ng* tekniği ile ağa çok fazla istek oluşturarak bağlı cihazların bağlantısını anlık olarak kesmektedir. Bağlantısı kopan cihaz otomatik olarak yeniden bağlanmayı denediğinde saldırgan şifre içeren veri paketini yakalayabilmektedir. Saldırgan için bir kez bağlantının kopup yeniden bağlanması durumu kablosuz ağ şifresinin ele geçirilmesine yeterlidir. Dolayısıyla kablosuz ağ bağlantısının kopması, normalin dışında bir durum olarak değerlendirilebilir.



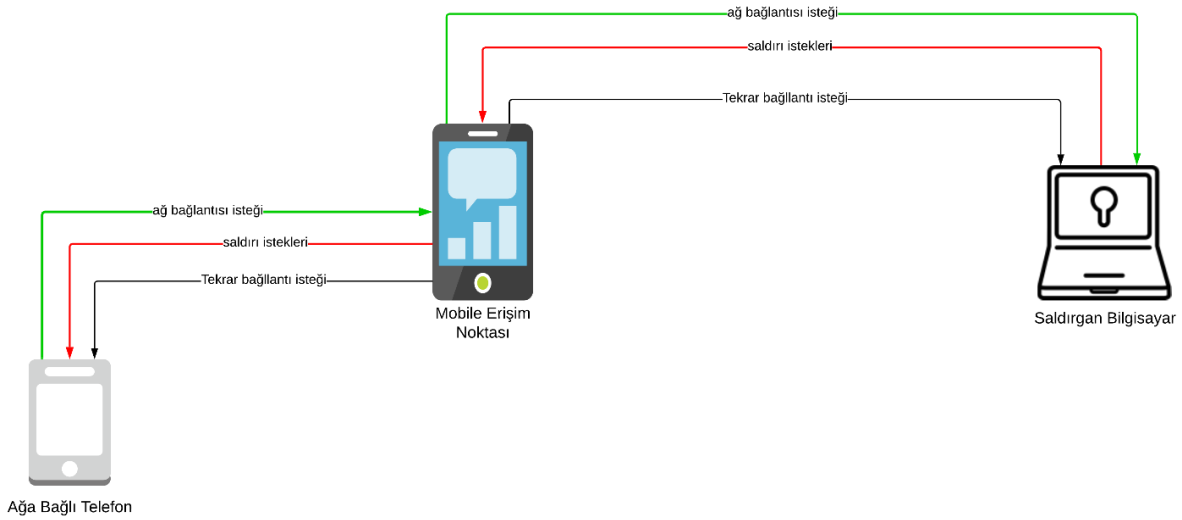
Şekil 24. Wireshark ile ağda şüpheli isteklerin tespiti

Bu bulgulara ulaşırken, Şekil 25'da blok diyagramı verilen bir mobil erişim noktası üzerinde test yapılmıştır. *Xiaomi Note 8 Pro* model *Android 10 işletim* sistemli telefondan internet paylaşım özelliği ile kablosuz erişim noktası oluşturulmuştur. Bu kablosuz ağa *Samsung S8+* model *Android 9* işletim sistemi olan telefon bağlı bulunmaktadır.



Şekil 25. Mobil erişim noktası simülasyon düzeneği

Şekil 26'de saldırgan bilgisayarın, mobil erişim noktasına bağlı kurban cihaza saldırısı anında gerçekleşen ağ isteği olayları görülmektedir. Buna göre öncelikle saldırı istekleri gelir ve ağa bağlı cihazın ağ bağlantısı kopar. Ağ erişimi kesilen cihazın ağa tekrar bağlanması için mobil erişim hizmeti veren cihaz etraftaki aynı frekansı ve kanalı dinleyen tüm kablosuz algılayıcı cihazlara tekrar bağlantı isteği gönderir. Bu istek ağ bağlantısı kopan kurban cihazın MAC adresi ile giden bir ARP isteğidir. Bu şekilde etraftaki cihazlara, bu MAC adresine sahip olup olmadıkları sorulmaktadır. Ağ bağlantısı kopan cihaz bu bağlantı isteğini aldığında, aranan MAC adresine sahip olduğu için cevap verecektir. Bağlantı isteği göndererek ağ şifresini içeren bir veri paketi göndererek ağa bağlanır. Saldırgan bilgisayar, bütün bu haberleşme trafiğini aynı kablosuz ağ frekansı ve aynı kanalda monitör modda dinlemekte ve bu süreçte şifre bilgilerini içeren veri paketini yakalayabilmektedir.



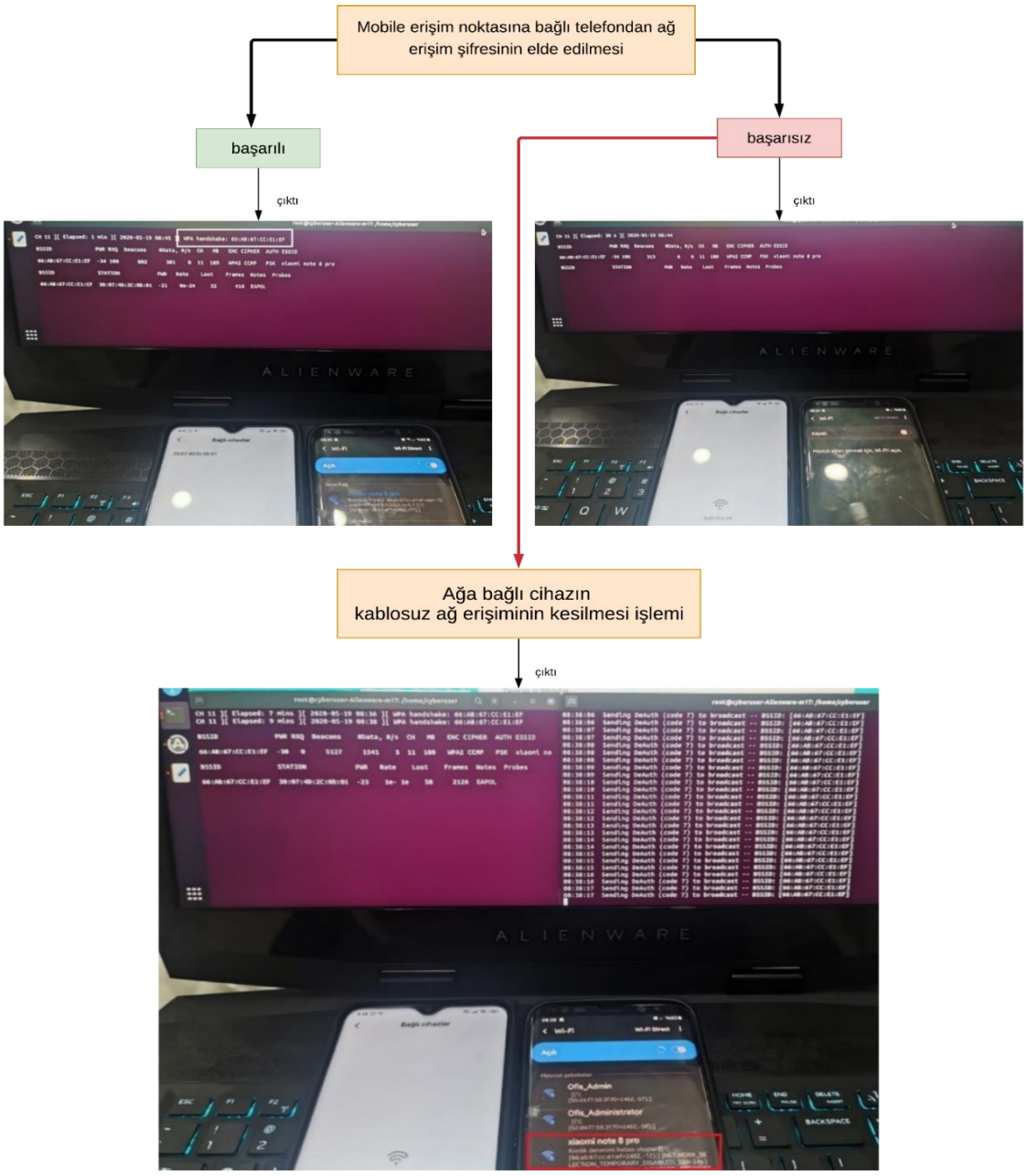
Şekil 26. Mobil erişim noktası üzerinden saldırı simülasyonu

Şekil 27'de görüleceği üzere, ağa bağlı bir cihaz bulunmadığında ya da ağa bağlı olup pasif durumda bekleyen bir cihaz olması durumunda (başarısız saldırı girişimi) saldırgan bilgisayar şifre içeren paketi yakalayamamıştır. Ağa bir cihazın bağlı ve bu cihazın aktif halde olması durumunda ise saldırının başarılı olduğu ve şifre içeren veri paketinin yakalandığı görülmektedir. Bazı durumlarda ağa bir cihaz bağlı olmasına rağmen saldırgan şifre paketini elde edememektedir. Ancak bu durumda bile saldırganın kablosuz ağ cihazının ve ağa bağlı kurban cihazın MAC adreslerini tespit ettiği saptanmıştır. Bu durum, Şekil 27'de *Ağa bağlı cihazın kablosuz ağ erişiminin kesilmesi işleminde* görülmektedir. Bu verilerden *BSSID* karşısında yazan değer, kablosuz ağ cihazının MAC adresidir. *STATION* karşısında yazan değer ise ağa bağlı olan ve şifre içeren veri paketinin yakalandığı cihazın MAC adresidir.

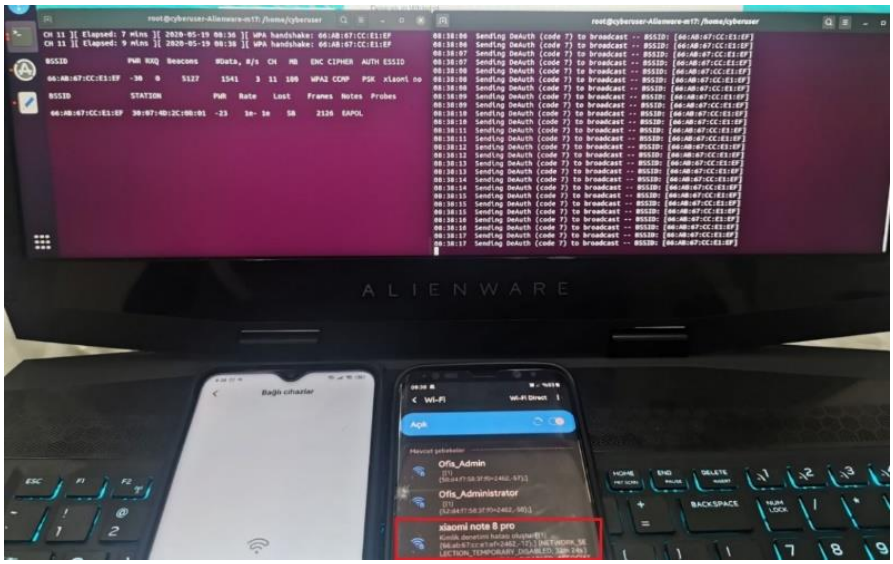
Şekil 28, saldırgan bilgisayar ağa bağlı bir cihaz bulunmasına rağmen şifre bilgisini içeren veri paketini yakalayamadığında gerçekleştirilen alternatif saldırıyı göstermektedir. Bu saldırı ile kablosuz ağa bağlı kurban cihazın bağlantısı kopartılarak yeniden bağlanma esnasında şifre içeren paketin elde edildiğini gösteren test sonucu verilmektedir. Yapılan test işleminde de görüldüğü gibi saldırıya uğrayan kablosuz ağa bağlı olan cihazda *kimlik denetim hatası* şeklinde bir bağlantı hatası oluşmaktadır. Dolayısıyla, saldırı anlarında cihazın bağlı olduğu ağdan kopacağı ve kimlik denetim hatası verebileceği bulgularına ulaşılmıştır.

Kablosuz ağa yapılan saldırılarla şifre tespitinin yanı sıra ağa bağlı cihazların erişiminin de engellenebileceği saptanmıştır. Eğer normalde sorunsuz kullanılan bir kablosuz ağa bağlantı sağlanamıyorsa, bu durum ilgili ağda o an bir servis reddi saldırısı gerçekleştiğine işaret edebilir. Yani alternatif olarak kullanılan bu saldırı, aslında bir DoS saldırısıdır. Ayrıca bazı durumlarda routerlerin aşırı yoğun doğrulama isteği nedeniyle kablosuz ağ cihazının ısınmasına hatta bozulmasına neden olduğu bilinmektedir.

[9] numaralı kaynakta, parola kırma yazılımları ile ağ üzerinden kablosuz ağ erişim elemanlarına aşırı yüklenilmesinden dolayı bu cihazların zarar görebileceği sonucu bildirilmektedir. Bu çalışmada da gerçekleştirilen şifre kırma deneme uygulamalarında işlem yoğunluğundan dolayı, cihazın aşırı ısınmaya bağlı olarak zarar görüp çalışmadığı gözlenmiştir.



Şekil 27. Wireshark ile ağda şüpheli ARP isteklerinin tespiti



Şekil 28. Kablosuz ağa erişimi kesme saldırısı

4.2 Linux Sunucu Sistemine Yapılan SSH Kaba Kuvvet Saldırısı

Yapılan araştırmalarda sunucu günlük (log) verilerinin kayıt altına alındığı dizinler incelenmiştir. SSH oturum başlatma kayıtları, */var/log/auth.log* dizininde tutulmaktadır. Bu dosya içerisinde her istek için olay bilgileri kayıt edilmektedir. Buradaki veriler analiz edilerek hangi işlemlerin başarılı hangi işlemlerin başarısız olduğu ve hangi IP adreslerinden saldırı geldiği gibi tespitler yapılabilmektedir.

SSH kaba kuvvet saldırı anlarının bir başka yansıması, oturum başlatma isteğinin SSH üzerindeki yoğun saldırılardan dolayı reddedilmesidir. Bu bulgu, konuyla ilgili bir saldırı yapılarak elde edilmiştir (Şekil 29). Eğer SSH kaba kuvvet saldırısı kullanıcı adını doğru tahmin ederek aralıksız ve çok fazla oturum başlatma isteği gönderirse, sisteme giremese de SSH girişini zorlaştırabileceği hatta bu isteklerin zaman aralıkları iyi organize edilmiş profesyonel bir saldırı yönetimiyle DoS saldırısı şeklinde hizmet dışı kalmaya sebebiyet verebileceği anlaşılmaktadır. Yani SSH kaba kuvvet saldırısının aynı zamanda SSH DoS saldırısına dönüşebileceği ortaya konulmuştur. Şekil 30'de görüleceği üzere, SSH DoS saldırısına uğrayan bir sunucuda oturum başlatma denemesi yapıldığında, '*kex_exchange_identification: Connection closed by remote host*' ya da '*kex_exchange_identification: Connection reset by peer*' bildirimi alındığı tespit edilmiştir. Çalışmada ulaşılan bulgulara göre, eğer SSH girişi anında bu uyarılar alınırsa bunun bir SSH hizmet reddi saldırısı olabileceği saptanmıştır.

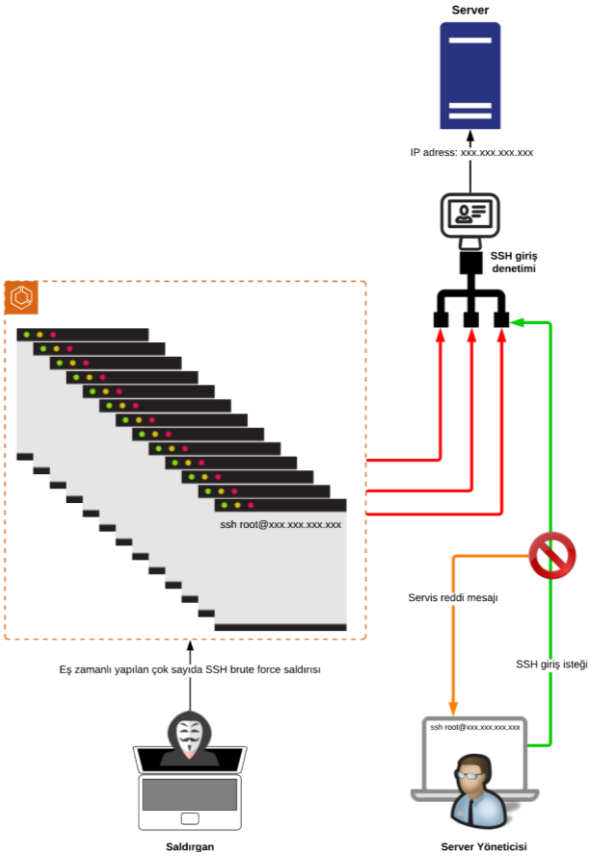
Şekil 29'deki simülasyonda yaklaşık 40 tane terminalden yerel sunucuda *root* kullanıcısına SSH kaba kuvvet saldırısı başlatılan ve her terminal penceresinde aralıksız olarak oturum başlatma isteği gönderilen örnek bir uygulama, Şekil 31'de verilmiştir. Sistem yöneticisi olarak başka bir terminal penceresi açılarak SSH oturum başlatma işlemi gerçekleştirilmek istendiğinde, bağlantı uzak masa üstü tarafından kapatıldı bildirimi alınmıştır.

SSH kaba kuvvet saldırılarının basit bir güvenlik duvarı komutu kullanarak saldırı gelen IP adresinin engellenmesi ile durdurulabileceği düşünülse de bu neredeyse etkisiz denebilecek bir tekniktir. Çünkü kaba kuvvet saldırısı yapan saldırganlar *Tor* ağı gibi birçok ağ üzerinden ve binlerce farklı IP adresi kullanarak saldırı yapabilmektedirler. Tam güvenlik için daha ileri düzey güvenlik duvarı komutları kullanılabilir. Çalışmada, SSH kaba kuvvet saldırılarına karşı *iptables* kuralları ile saldırı önleme uygulaması yapılmıştır. Elde edilen sonuçlara göre iyi organize edilmiş bir güvenlik duvarının oldukça yüksek güvenlik sağlayabileceği anlaşılmıştır.

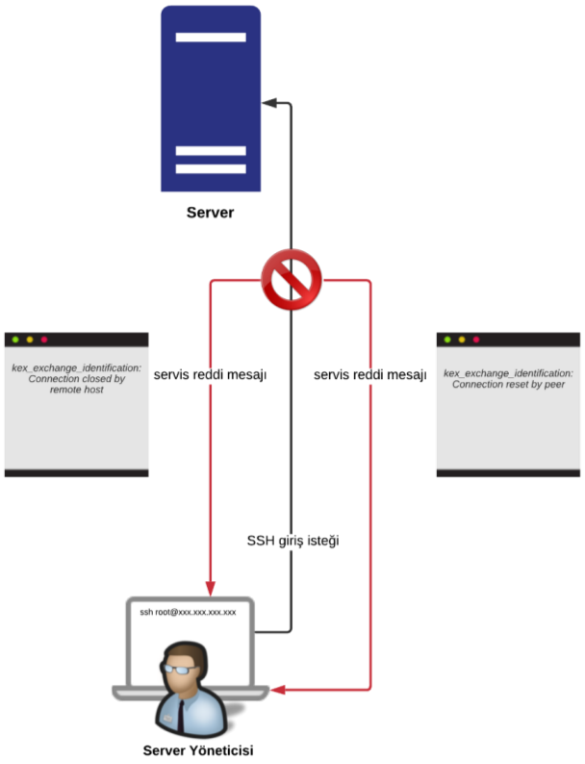
Şekil 33'de görüleceği üzere, gerekli *iptables* kuralları girildikten sonra */sbin/iptables-save* komutu ile kayıt edilip yürürlüğe sokulmaktadır. Bu kurallar yürürlüğe girer girmez ilk yaptığı faaliyet, saldırgan IP adresini SSH sunucusundan düşürmek olmuştur. Elde edilen bulgular ışığında amaçlanan sonuca ulaşılmıştır.

4.3 SSH Kaba Kuvvet Saldırısının İlişkisel ve Anlık Raporlarının Elde Edilememesi

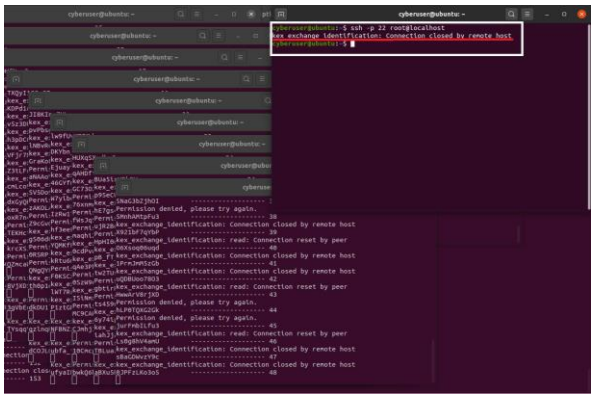
SSH kaba kuvvet saldırılarının ilişkisel ve anlık olarak raporlama sorununa ilişkin yapılan testlerde ELK SIEM sistemi kullanılmıştır. ELK-SIEM sisteminde *failed* etiketli raporlar ile sunucuya başarısız SSH login girişi yapıldığı raporlanır. Birbirleriyle ilişkili SSH oturum başlatma denemelerini içeren raporlar anlık olarak *Kibana* panelinde incelenmiştir (Şekil 34). Buna göre; çok kullanılan standart kullanıcı isimleri denenerek saldırı yapıldığı tespit edilmiştir. Bu raporun detayı saldırgan IP adresini ve SSH port numarasını doğru tahmin etmiş olmasıdır. En çok saldırının geldiği kaynak Çin tabanlı IP adresleridir ve onu sırasıyla Almanya ve Amerika'nın takip ettiği tespit edilmiştir.



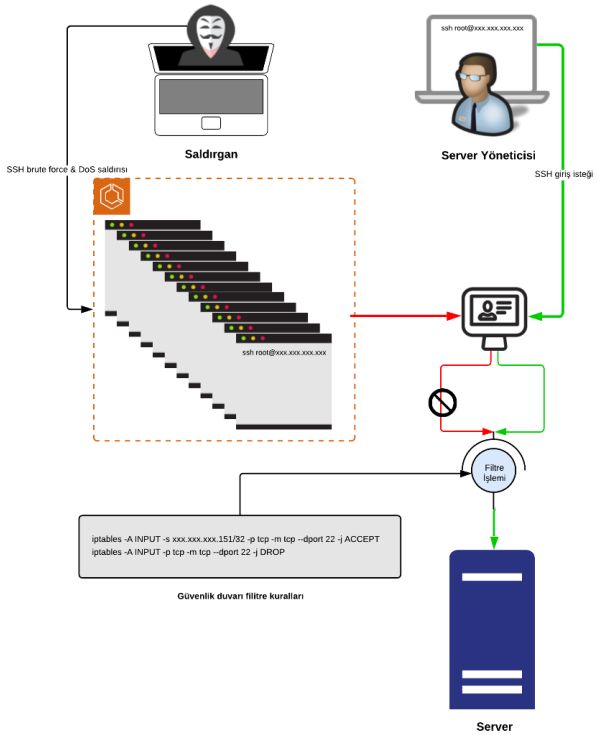
Şekil 29. SSH kaba kuvvet ve SSH servis reddi saldırısı modeli



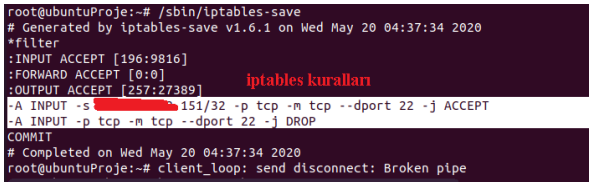
Şekil 30. Servis reddi saldırısı anında alınan SSH login hata bildirimleri



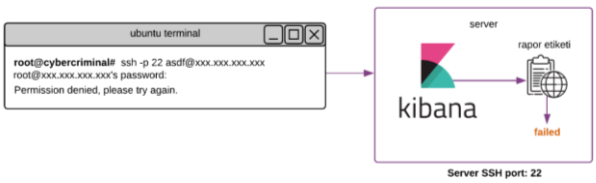
Şekil 31. SSH DoS saldırısına uğrayan sunucu sisteminin servis dışı mesajı



Şekil 32. Sistem yöneticisi dışındaki bütün IP adreslerinin port erişiminin engellenmesi

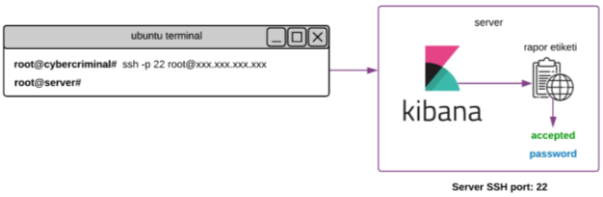


Şekil 33. Sistem yöneticisi dışındaki bütün IP adreslerinin portuna erişiminin engellenmesi



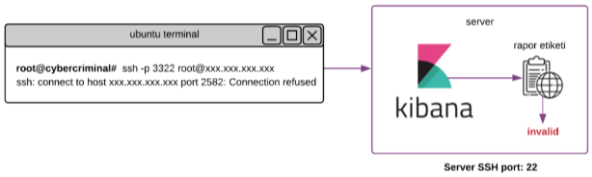
Şekil 34. ELK-SIEM ile *failed* etiketli saldırı tespiti

ELK-SIEM sisteminde *accepted* ve *password* etiketleri, sunucuya gelen SSH oturum açma isteklerinden başarılı olduğunu ve giriş isteği için password yöntemi kullanıldığını raporlar (Şekil 35). Başarılı SSH oturum açma olayının tanınmayan bir IP adresi tarafından gerçekleştirilmiş olması, sunucu şifresinin tespit edildiği anlamına gelmektedir.



Şekil 35. ELK-SIEM ile *accepted* ve *password* etiketli saldırı tespiti

ELK-SIEM sisteminde *Invalid* etiketli raporlar ile geçersiz oturum başlatma denemeleri bildirilmektedir (Şekil 36).



Şekil 36. ELK-SIEM ile *invalid* etiketli saldırı tespiti

Invalid etiketli raporlar incelendiğinde, saldırı metodunda *Password* kullanılmadığı görülmüştür. *Failed* etiketi ile sunulan başarısız oturum başlatma denemesinde dahi şifre metodu olarak *password* kullanılmışken *Invalid* etiketi ile raporlanan olaylarda kullanılmaması, saldırı denemesinin SSH portuna ulaşamamış olmasını düşündürmektedir. Yapılan testlerde SSH port numarası hatalı şekilde yazılıp oturum başlatma denemesi gerçekleştirildiğinde, ELK-SIEM sisteminde *Invalid* etiketi ile hata raporu bildirildiği görülmüştür. Bu tespitler ışığında, *Invalid* etiketi ile gelen isteklerin, sunucu üzerinde standart numarası değiştirilmiş SSH portunu tespit etmeye yönelik istekler olma ihtimalinin yüksek olduğu sonucuna varılmıştır.

ELK-SIEM sisteminde *message* etiketi ile bildirilen bir başka rapor da önemli saldırı istihbaratları barındırmaktadır. Bu raporlardan elde edilen veriler alınacak tedbirler açısından önemlidir. *Message* etiketi ile raporlanan SSH oturum başlatma denemeleri, peş peşe 3 kez hatalı giriş yapan IP adreslerinin raporlarını içerir. Bu hatalı girişten kasıt, kullanıcı ismini ve port numarasını doğru tahmin ederken sadece şifreyi hatalı giren SSH isteklerdir. Eğer bu istekler sistem yöneticisinin bilgisi dâhilinde değilse, doğrudan sunucuya odaklanmış kasıtlı bir saldırı olması muhtemeldir. Örneğin bir SSH DoS saldırısı gerçekleşecek olursa, bu saldırı *message* etiketi ile raporlanacaktır. Bu sebeple diğer oturum başlatma isteklerine nazaran daha ciddi ataklara ait verilerin *message* etiketi ile raporlandığı saptanmıştır. Bu şekilde tespit edilmiş saldırı girişimlerini gerçekleştiren IP adreslerinin, SSH portuna erişiminin engellenmesi önerilmektedir. Ayrıca kritik saldırı raporlarından hemen haberdar olunması için SIEM sisteminde alarm üretilmesi ve bunun bir mail yoluyla ya da bildirim yoluyla uyarı iletecek şekilde ayarlanması da önemlidir.

Şekil 37. ELK-SIEM sisteminde *message* etiketi saldırı tespiti

V. TARTIŞMA VE ÖNERİLER (DISCUSSION AND SUGGESTIONS)

5.1 Kablosuz Ağlara Yapılan Saldırıların Tespitine Yönelik Öneriler

Kablosuz ağlara gelen saldırıların tespit edilebilmesi için belirli zaman ve periyodlarda kablosuz ağ trafiğinin Wireshark gibi kablosuz ağ trafiğini dinleyen yazılımlarla anormal veri trafikleri olup olmadığını araştırmak maksatlı kontrol yapılması önerilir.

Kablosuz ağa erişim sağlamış yabancı cihazların tespiti için Nmap, Netdiscover ya da Wireshark gibi ağ üzerinde analiz işlemleri yapabilen yazılımlar kullanılarak kontrol edilmesi önerilir.

Ağa bağlı olan bütün cihazların gerçek zamanlı ve kesin sonuçlarla elde edilebilmesi için kablosuz ağ cihazının güvenlik duvarı panelindeki cihaz erişim loglarının kontrol edilmesi önerilir.

Mutlaka güvenlik duvarı olan bir kablosuz ağ cihazı kullanılması önerilir. Öte yandan birinci nesil güvenlik duvarı teknolojisi, bugünün internet suçluları tarafından gönderilen zararlı ağ paketlerini denetlemek ve olası saldırılardan korumak için yetersiz hale gelmiştir [15]. Bu nedenle, sistem ihtiyacına uygun yeni nesil güvenlik duvarları kullanılması tavsiye edilmektedir.

Kablosuz ağ şifre kırma saldırılarında şifrenin başarılı şekilde tespit edilmesi durumuna karşı router güvenlik duvarı ayarlarında sadece bilinen MAC adreslerine ağ erişim yetkisi verilmesi önerilir.

Ağa bağlı cihazların ağ erişimi kopartıp ağa bağlanmasını engellemeye yönelik gerçekleştirilen DoS saldırılarına karşı kablosuz ağ cihazının görünürlüğü gizliye alınması önerilmektedir.

Ağ cihazları, ağ alt yapısı tarafından gerçekleştirilen işlemler ile ilgili günlük (log) dosyalarını saklamaktadırlar. Bu kayıtlar, güvenlik zafiyetlerinin belirlenmesinde ve önlem alınmasında büyük önem taşımaktadır. Cihaz ara yüzlerinin durum değişikliği, sistem yapılandırma değişikliği, erişim listelerine takılan bağlantılar gibi güvenlik açısından önemli olan bilgilerin kaydı titizlikle incelenmelidir [5].

Özel karakterler içeren uzun şifreler seçmek, sözlük atak saldırılarında tespiti zorlaştırmaktadır. Bu yüzden en az 8 karakterli ve içerisinde büyük harf, küçük harf, rakam ve özel karakter bulunan şifreler kullanılması önerilmektedir.

Kullanılan ağ erişim şifreleri Google Zoom gibi şifre bilgileri çalınan ya da 3. taraf güvensiz bazı sitelerde daha önce kullanılmış şifrelerin aynısının kullanılmaması önerilmektedir. Çünkü sözlük atak saldırılarında kullanılan şifre sözlüğü bu tarz yerlerden elde edilmiş şifrelerdir.

5.2 Kablosuz Ağlara Yapılan Saldırıların Önlenmesine ilişkin Değerlendirmeler

Kablosuz ağlara yapılan saldırıların tespiti ve önlenmesine yönelik yapılan araştırma konusunda elde edilen sonuçlar, araştırma açısından önemli sonuçlardır. Araştırmanın amacı kablosuz ağlara yapılan saldırıların tespiti ve önlenmesi üzerine bir saldırı simülasyonu araştırmasıdır. Elde edilen sonuçlar amaca uygun şekilde hizmet etmiş ve amaçlanan hedefler gerçekleştirilmiştir.
Literatürde incelenmiş olan yeni saldırı yazılımları da araştırma konumuz olan kablosuz ağ güvenlik protokolü olan WPA-WPA2 algoritmaları ile gelen aynı zafiyetleri sömürmektedir. Saldırı aşamaları bakımından aynı teknik adımlar izlenmekte ve benzer sonuçlar elde edilmektedir. Dolayısıyla elde edilmiş sonuçlar benzer çalışmalar ile tutarlıdır ve yapılan araştırma açısından önemlidir.

Bilimsel katkı olarak ele alındığında, yapılan çalışmada yeni bir savunma tekniğinden ziyade mevcut bilinen savunma teknikleri organize edilerek gerçek simülasyon ortamı ile daha kapsamlı şekilde saldırıların yan etkileri analiz edilerek uygulamaya dönük bir çözüm literatüre sunulmuştur.

Bu simülasyon çalışmasında kablosuz ağ ortamında yapılan testler ve araştırmalar sonucunda savunma teknikleri belirlenmiştir. Belirlenen çözüm teknikleri ile probleme karşı gerekli tedbir ve kurallar belirlenip uygulanarak oldukça yüksek koruma sağlayacak bir sonuç elde edilmiştir. Yapılan çalışmanın en önemli katkılarında birisi araştırma çalışmasında sadece metodolojik değil uygulamalı olarak gerçek ortamlarda simülasyon işlemleri ile yapılmış olmasıdır. Bu sayede uygulamaya dönük bilimsel araştırma çalışmaları için çok daha değerli olacağı düşünülmektedir.

5.3 SSH Kaba Kuvvet Saldırı Tespitine Yönelik Öneriler

Bir SSH kaba kuvvet saldırısının gerçekleşebilmesi için asgari gereklilik, saldırganın SSH port numarasını ve kullanıcı ismini doğru tahmin etmesidir. Dolayısıyla bunların tahmin edilmesi kolay olmayacak şekilde değiştirilmesi önerilmektedir.

Port numaraları değiştirilmesine rağmen sunucu sisteminin ağı üzerindeki açık portlarını tarayarak tespit işlemi yapmayı deneyen saldırılar bulunmaktadır. Bilindiği üzere root kullanıcısı her Linux sunucu sisteminde standarttır. Dolayısıyla root kullanıcısına yönelik SSH kaba kuvvet saldırısı devam edecektir. Bu saldırının önlenmesi için saldırının geldiği IP adresinin SSH portuna erişimi engellenmesi önerilir.

Eğer web hizmeti sunulan bir sunucuya saldırı geliyorsa saldırı gelen IP adreslerinin sadece SSH portuna engellenmesi tavsiye edilir. Çünkü saldırı gelen IP adresi VPN sunucusu ya da normal bir ülkenin internet çıkış IP adresi olabilir. Aksi takdirde barındırılan web sitelerinin ziyaretçileri yapılan engellemeden dolayı olumsuz etkilenebilirler.

Eğer SSH kaba kuvvet saldırıları çok fazla IP adresinden geliyorsa, en kesin çözüm olarak sistem yöneticilerinin erişim sağladığı IP adresleri dışındaki bütün IP adreslerinin sunucu SSH portuna erişimi engellenmesi önerilir.

Genellikle saldırılar Tor ağı gibi internet ağlarından gelmektedir. Dolaysıyla tek tek binlerce IP adresinin saldırı yaptıkça engellenmesi işlemi yerine, Tor IP adreslerinin listesi çıkartılıp topluca SSH portuna erişimlerinin engellenmesi seçeneği de önerilmektedir.

5.4 SSH Kaba Kuvvet Saldırıların Çözümüne İlişkin Değerlendirme

SSH kaba kuvvet saldırılarının tespiti ve önlenmesi çalışmasında yapılan simülasyonlar incelenerek saldırının tespiti ve önlenmesine yönelik teknikler oluşturulmuş ve başarılı şekilde uygulanmıştır. Yine bu araştırma çalışmasında elde edilen sonuçlar amaca hizmet ettiği için başarılı ve önemli olduğu kabul edilir. Araştırma çalışması konuyla ilgili literatürde yer alan önceki çalışmalar ile tutarlıdır. Zaten SSH kaba kuvvet saldırısının ve SSH DoS saldırılarının temelleri normal ssh oturum açma isteğinin kötü niyetli kullanılarak yapılmasıyla gerçekleştirilir. Dolayısıyla günümüzde hala bu saldırılarda sömürülen zafiyet aynıdır. Günümüzdeki güncel saldırı ve önleme teknikleri yapılmakta olan bu çalışma ile paralel ve tutarlıdır.

Günümüzde siber saldırıların sömürdükleri zafiyetler benzer açıklıklardır fakat bunların kullandıkları kanallar farklılık göstermektedir. Ayrıca günümüzde saldırılara karşı gelişmiş SIEM sistemleri kullanılmaktadır. Yapılan çalışmada da zaten SIEM sistemleri tespit ve önleme aşamalarında kullanılmıştır.

Sonuç olarak yapılan bu çalışma günümüzdeki yeni saldırı ve savunma teknikleri açısından güncel ve önemli bir çalışmadır.

Sunucu yöneticisi ve diğer sistem kullanıcıları IP adresleri dışındaki bütün IP adreslerinin engellenmesi bazı durumlarda kullanışlı olmayabilir. Örneğin birçok şirket VPN bağlantıları ile çalışmaktadır ve bu nedenle de kullanıcıların IP adresleri sürekli değişebilmektedir. Bu durumlarda alınan güvenlik tedbirleri kullanışlı olmayacaktır. Bu yüzden daha ileri bir araştırma ile farklı çözüm yöntemleri oluşturulması gerekebilir.

Bilimsel katkı olarak ele alındığında, yapılan çalışmada gerçek ortamlarda bir simülasyon ortamı hazırlanarak gerçekleştirilen testler ve araştırmalar sonucunda SSH kaba kuvvet ve servis reddi saldırılarına karşı yöntemler geliştirilmiştir. Bu çalışma aynı problemler hakkında yapılacak başka araştırmalar için yol haritası niteliğinde örnek bir araştırma modeli olarak literatüre sunulmuştur. Uygulamalı simülasyon çalışmaları literatürde az bulunması ve metodolojik anlatımların uygulama aşamasında yetersiz kalması nedeniyle yapılacak benzer uygulamalı araştırmalar için önemli bir yardımcı çalışma olacaktır.

5.5 SIEM Sistemleri ile Saldırı Tespit ve Önlenmesine Yönelik Değerlendirme ve Öneriler

ELK-SIEM saldırı raporlarında ‘message - invalid’ etiketiyle raporlanan saldırıları gerçekleştiren IP adreslerinin, SSH portuna erişiminin engellenmesi önerilir

SSH kaba kuvvet saldırılarının tespitinde ve önlenmesinde, gerçek zamanlı tehdit istihbaratı sağlayan, anlık saldırı raporları sunan ve alarm bildirimi üretilebilen alternatif SEIM sistemlerinin de kullanımı önerilir. SIEM sistemleri arasında en çok kullanılanlardan SPLUNK, bu alanda kullanım için tavsiye edilmektedir.Kritik saldırı raporlarından hemen haberdar olunması için SIEM sisteminde alarm üretilmesi ve bunun bir mail yoluyla ya da bildirim yoluyla uyarı iletecek şekilde ayarlanması önerilir. ELK-SIEM saldırı raporlarında ‘failed’ etiketiyle raporlanan saldırıları gerçekleştiren IP adreslerinin, SSH portuna erişiminin engellenmesi önerilir

Kaba kuvvet saldırılarının gerçek zamanlı olarak saldırı raporları elde edilmesi ve ilişkisel raporların oluşturulması işlemi, yapılan simülasyonlarda başarılı şekilde gerçekleştirilmiş ve saldırı raporları incelenmiştir. SIEM sistemleri ile elde edilen verileri kullanarak, saldırılar hakkında daha detaylı yorumlar yapılabilmiştir. Ayrıca saldırıların anlık olarak tespit işlemleri de yapılabilmiştir. Dolayısıyla araştırma amacına ulaşmıştır ve sonuçlar yapılan çalışma için önemlidir.

Elde edilen sonuçlar daha ileri düzeylerde ve farklı ortamlarda ELK-SIEM sistemi ile yapılacak analiz çalışmalarında da geçerlidir. Çünkü ELK-SIEM sistemi log dosyalarındaki davranışları kendi sistemindeki korelasyonlara göre yorumlamaktadır. Dolayısıyla ELK-SIEM yazılımında standart korelasyonlar kullanıldığı takdirde, farklı ortamlarda da aynı sonuçlar elde edilmektedir.

Türkçe literatürde SIEM konusu ile ilgili birkaç satırdan öteye geçmeyecek kadar sınırlı içerik bulunmaktadır. Ayrıca İngilizce literatürde de SIEM konusuyla ilgili oldukça sınırlı sayıda çalışma bulunmaktadır. Bu yüzden çalışmadaki kapsamlı ve detaylı şekilde ve uygulamalı olarak yapılan SIEM tabanlı analiz ve incelemelerin literatüre katkı bakımından önemli olacağı düşünülmektedir.

Günümüzde gelişen teknikler sebebi ile ve bir takım saldırı kitleri ile saldırılar yapılabilmektedir. Bu durum, siber güvenlik tekniklerinden daha hızlı gelişmekte olan siber saldırılarla ilgili yapılacak savunma, tespit ve önleme mekanizmaları için yapay zekâ tabanlı uygulamaların kayda değer başarı sağlayacağını göstermektedir. Bu nedenle gelecek çalışmalarda, yapay zekâ destekli saldırı tespit ve savunma uygulamaları üzerinde durulması düşünülmektedir.

Bilimsel katkı olarak ele alındığında, makale çalışmasının en önemli katkılarından birisi SIEM yazılımı ile gerçek sunucu ortamında simülasyon yapılarak SSH kaba kuvvet saldırılarının tespiti ve raporlarının analizlerinin yapılmasıdır. Bu şekilde SIEM yazılımlarının önemine yönelik farkındalık sağlanmıştır. Yol haritası niteliğindeki bu çalışma ile mevcut sorunlar çözülebilecek ve bu çözüm yolları geliştirilebilecektir. Ayrıca ELK-SIEM yazılımı içinde, SSH oturum açma istekleri sonucu oluşan olaylar incelenmiştir. SIEM yazılımı yönetim panelinde SSH login olayları raporunda bulunan etiketlerin hangi anlamlara geldiği detaylı olarak incelenmiş ve analizi yapılmıştır. Yine bu alanda literatüre, literatürde olmayan SIEM sistemi ile SSH kaba kuvvet saldırılarının anlık tespitine yönelik, yol haritası niteliğinde bir deneysel simülasyon çalışması kazandırılmıştır.

VI. SONUÇ VE DEĞERLENDİRMELER (CONCLUSION and EVALUATIONS)

Bu çalışmada, kablosuz ağlara yapılan şifre kırma saldırıları, Linux tabanlı sunucu sistemlerinde SSH kaba kuvvet saldırıları ve Linux tabanlı sunucularda SSH kaba kuvvet saldırılarının SIEM ile tespit edilip raporların analizi şeklinde üç ana konuya yoğunlaşılmıştır. Her bir başlık altında ayrı ayrı deney ve test ortamları oluşturularak örnek olay incelemesi şeklinde elde edilen sonuçlar yorumlanmıştır. Saldırıların hangi durumlarda başarıya ulaşabileceği, belirtilerinin neler olduğu ve nasıl tespit edilebileceği, nasıl önlenebileceği gibi bir dizi bulgular sunulmuştur.

Ayrıca bu araştırma ön görülenin dışında farklı etkilerinde keşfedilmesine olanak sağlamıştır.
Elde edilen bulgularla makalede incelenen siber saldırılara karşı etkili çözümler alınabilmektedir fakat daha esnek sistem kullanımı gerektiren işler için bu ve buna benzer çalışmalara ihtiyaç duyulmaktadır. Gerekli durumlarda yapılacak yeni çalışmalar için bu simülasyon çalışmaları bir yol haritası niteliğinde olacaktır.

Saldırgan kablosuz ağa saldırı gerçekleştirdiği sırada Wireshark programı ile ağ üzerindeki trafik incelendiğinde, kablosuz ağda peş peşe çok sayıda ARP isteği oluştuğu tespit edilmiştir. Kablosuz ağa saldırı yapan cihazın MAC adresi veya cihaz model ismi tespit edilememektedir. Saldırının geldiği cihaz bilinmezliğini korumaktadır. Saldırılar bir cep telefonunun mobil erişim noktası ve bir routeri cihazının kablosuz ağı üzerinde test edilmiştir. Yapılan testlerin her ikisinde de saldırgan menzilindeki kablosuz ağ cihazlarıyla, aynı frekansta ve aynı kanala yerleşerek ağ trafiğindeki veri paketlerini ele geçirebilmektedir. Kablosuz ağ şifreleri basit zayıf şifreler olduğunda WPA - WPA2 gibi her ne kadar güvenli şifreleme algoritmalarına sahip bir kablosuz ağ kullanılmış olsa da saldırgan sözlük atak saldırılarıyla bu şifreleri kırabilmektedir. Şifre kompleksliği arttırıldığında şifre içeren veri paketindeki şifre çözülememektedir.

Başarılı kablosuz ağ saldırıları kablosuz ağ güvenlik duvarı log kayıtları incelenerek tespit edilebilmektedir. Yapılan saldırı tespiti neticesinde SSH kaba kuvvet saldırılarını önlemek için saldırı gerçekleşen IP adreslerinin engellenmesi amacıyla betik komutları belirlenmiştir.

Çok sayıda IP adresi üzerinden saldırı alan sistemler için kullanıcıların IP adresi dışındaki bütün IP adresleri SSH girişine kapatılmıştır. Bu yöntemle SSH kaba kuvvet saldırılarında kesin çözüme ulaşıldığı sonucuna varılmıştır. Yapılan saldırı simülasyonu işleminde, çok sayıda terminalden SSH kaba kuvvet saldırısı işlemi başlatıldığında SSH servis reddi saldırısına sebep olduğu sonucuna ulaşılmıştır.

SSH kaba kuvvet saldırılarının gerçek zamanlı ve ilişkisel raporlarının oluşturulması konusunda yapılan simülasyon çalışmasında ELK-SIEM yazılımı kullanılmıştır. Gerçek zamanlı saldırı raporları ELK-SIEM yazılımı ile başarılı şekilde oluşturulmuştur. Elde edilen sonuçlar incelenerek hangi saldırıların başarılı olduğu ve hangilerinin riskli saldırı grubunda olduğu analiz edilerek açıklanmıştır. ELK-SIEM yazılımında sunulan raporlarda SSH kaba kuvvet saldırıları için 'message' etiketi ile gelen saldırılar doğrudan sunucu sistemini hedef almaktadır. Bu nedenle SSH oturum açma işlemlerinde DoS saldırısına neden olabileceği için önemli risk taşıdığı sonucuna varılmıştır. 'invalid' etiketi ile raporlanan saldırılar aynı IP adresinden çok fazla kez tekrar ediliyorsa. Bu saldırıların ssh port taraması yaptığı sonucuna varılmıştır. 'accepted' etiketi ile raporlanan IP adresleri, eğer yöneticiye ya da alt kullanıcılara ait bir IP adresi değilse bu başarıya ulaşmış bir SSH kaba kuvvet saldırısı olacağı sonucuna varılmıştır.

Sunulan bu çalışmanın geliştirilmesine yönelik gelecek çalışmalar olarak kablosuz ağa gerçekleştirilen şifre kırma saldırılarında, kablosuz ağa tekrarlı şekilde ARP doğrulama isteği gönderilerek ağa bağlı cihazların ağ erişiminin kesilmesini önlemek için ARP protokolünde yeni lokal ve küresel ölçekte geliştirmeler yapılabilir. Örneğin TCP seli saldırılarında TCP protokolünde yapılan geliştirmeler ile saldırılar önlenmiştir.

Güvenlik duvarı kurallarının farklı ihtiyaçlara göre geliştirilmesi, örneğin sadece tek IP adresine izin verilen bir savunma politikası, değişken IP adresleri üzerinden oturum açma işlemi gerektiren durumlarda işlevsel olmayacaktır. Bu tarz durumlarda savunma protokollerinin görevlerini icra edebilmesi için ya dinamik kurallara sahip bir güvenlik duvarı oluşturulması gereklidir ya da bu ihtiyaçları karşılayacak yeni bir sunucu mimarisi oluşturulabilir.

SSH giriş istekleri bütün IP adreslerine açık hale getirilerek SIEM sistemleri ile şüpheli isteklerin tespiti ve önleme denetimi yapılarak proje çalışması geliştirilebilir. SIEM sistemleri ile yerel internet ağında kablosuz ağ erişim cihazı log kayıtları incelenerek ilgili paket istekleri için saldırı alarmları oluşturulabilir. Yakın gelecekte yapay zeka destekli siber saldırılara karşı değişen kompleks olaylarla ilgili yorum çıkartıp kararların hızlı şekilde uygulanması gerekli olacaktır. Bu gibi durumlar için bu projenin geliştirme çalışması olarak SIEM sistemlerinin bir yapay zeka yazılımı ile birlikte kullanılabileceği daha ileri seviyeli çalışmaların yapılması planlanmaktadır.

KAYNAKLAR (REFERENCES)

[1] Kara, İ . (2019). Kaba Kuvvet Saldırı Tespiti ve Teknik Analizi. Sakarya University Journal of Computer and Information Sciences, 2 (2) , 61-69 . DOI: 10.35377/saucis.02.02.561844

[2] Arıkan, S. M., Benzer, R. (2018). Bir Güvenlik Trendi: Bal Küpü. Acta Infologica, 2(1), 1-11.

[3] Baykara, M., Daş, R. (2019). Saldırı tespit ve engelleme araçlarının incelenmesi. Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi, 10(1), 57-75.

[4] Durmuş, G., Soğukpınar, İ. (2019). İkili Yürütülebilir Uygulamalarda Arabellek Taşması Zayıflığına Neden Olan Şüpheli İkili İşlem Kod Dizilimlerinin Tespiti. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 13(1), 11-19.

[5] Baykara, M., Daş, R., Tuna, G., (2016). Web Sunucu Erişim Kütüklerinden Web Ataklarının

Tespitine Yönelik Web Tabanlı Log Analiz Platformu. Fırat Üniversitesi Mühendislik Bilimleri Dergisi, 28(2), 291-302.

[6] Tan, H., Aktaş, Z. (2011). Bir Kuruluşun Bilgi Sistemi Güvenliği İçin Bir Yaklaşım. TMMOB EMO Ankara Şubesi Haber Bülteni, 2011/5, 16-21.

[7] Akbal, E., Ergen, B. (2019). Kablosuz Yerel Alan Ağlarında Yapay Bağışıklık Sistemi ile Saldırı Tespiti ve Performans Analizi. http://www.emo.org.tr/ekler/8947fab05bee9c5_ek.pdf, Erişim Tarihi: 17.04.2020.

[8] Gezgin, D. M., Buluş, E. (2012). Kablosuz Ağların Güvenlik Açıklarının Eğitim Amaçlı İncelenmesi İçin Uygulama Tasarımı. Trakya Üniversitesi Eğitim Fakültesi Dergisi, Cilt 2 Sayı 1, 127-135.

[9] Gündüz, M. Z., Daş, R. (2014). Kablosuz Yerel Alan Ağlarına Sızma Uygulaması ve Temel Güvenlik Önerileri. 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 295-300.

[10] Gezgin, D. M., Buluş, E. (2013). Kablosuz Ağlar İçin Bir DoS Saldırısı Tasarımı. Bilişim Teknolojileri Dergisi, 6(3), 17-23.

[11] Akbal, E., Doğan, Ş., Tuner, T., Atalay, N. S. (2019). Adli Bilişim Alanında Ağ Analizi. Bitlis Eren Üniversitesi Fen Bilimleri Dergisi, 8(2), 582-594.

[12] Karaağaçlı, E. S., Müngen, A. A., Erdöl, H. (2016).). PCAP Paketler ile Restfull API'yi Gerçek Zamanlı Dinlemek. Yönetim Bilişim Sistemleri Dergisi, 2(2), 150-156.

[13] Karadoğan, İ., Daş, R., Baykara, M. (2013). Scapy ile ağ paket manipülasyonu. 1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu, 20-21.

[14] Kartal, M., Sağıroğlu, Ş., Bülbül, H. İ. (2013). IPV6'da Güvenlik Açıklarına Genel Bir Bakış. Politeknik Dergisi, 16(3), 119-127.

[15] Küçüksille, E. U., Yalçınkaya, M. A., Uçar, O. (2014). Siber saldırılarda istismar kitlerinin kullanımı üzerine bir analiz ve savunma önerileri. 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 17-18.