T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

LİNUX SİSTEMLER İÇİN DERİNLEMESİNE ADLİ ANALİZ YAPILARAK KALICILIK YAPILARININ TESPİT EDİLMESİ

Büşra AYTEKİN

Yüksek Lisans Tezi

ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI

Adli Bilişim Mühendisliği Bilim Dalı

TEMMUZ 2022

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

LİNUX SİSTEMLER İÇİN DERİNLEMESİNE ADLİ ANALİZ YAPILARAK KALICILIK YAPILARININ TESPİT EDİLMESİ

Tez Yazarı
Büşra AYTEKİN

Danışman
Doç. Dr. Fatih ERTAM

TEMMUZ 2022
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Linux Sistemler için Derinlemesine Adli Analiz Yapılarak Kalıcılık Yapılarının Tespit Edilmesi
Yazarı:	Büşra AYTEKİN
İlk Teslim Tarihi:	04.06.2022
Savunma Tarihi:	04.07.2022

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

		İmza
Danışman:	Doç. Dr. Fatih ERTAM Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Başkan:	Prof. Dr. Ömür AYDOĞMUŞ Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Üye:	Dr. Öğr. Üyesi İbrahim Rıza HALLAÇ Alanya Alaattin Keykubat Üniversitesi, Mühendislik Fakültesi	Onayladım

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Kürşat Esat ALYAMAÇ
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Linux Sistemler için Derinlemesine Adli Analiz Yapılarak Kalıcılık Yapılarının Tespit Edilmesi " Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

04.07.2022

Büşra AYTEKİN

ÖNSÖZ

Son yıllarda siber saldırıların her türlü elektronik ortamı hedef içerisinde bulundurduğu ve vakaların çözüm sürecinin uzamasının sisteme vermiş olduğu tahribatı artırmış olduğu tespit edilmiştir. Bu nedenle gelişmiş yönetimli müdahale ürünleri kullanılarak yapılan hızlı incelemeler sonucu Windows sistemlerden adli delil elde etme süreçleri yaygınlaşmış ve daha kolay iken, Linux sistemlerden elde edilen delillerin incelenmesi ve Linux sistemlerde saldırı vektörlerinin açık şekilde belirlenmesi daha sınırlı yöntemler sonucunda oluştuğundan konu özelinde araştırma yapılması gerekliliği motivasyon oluşturmuştur.

Adli bilişim, siber suçla ilgili her türlü elektronik cihaz içerisinde bulunan verilerin gerektiğinde mahkemelerce delil olarak kabul edilecek şekilde kurtarılmasına ve araştırılmasına, inceleme yapıldıktan sonra raporlanmasına odaklanan bir süreçtir. Elektronik cihazlar arasında; bilgisayarlar, ağ, bulut, sabit sürücü, sunucu, telefon veya altyapıya bağlı herhangi bir uç nokta sistemi bulunur. Ayrıca, e-posta, SMS, resim/video, silinen dosyalardan ve çok daha fazlasından bilgi toplamayı amaçlayan süreçtir. İşletim sistemi özelinde saldırı göstergelerinin tespit edilmesi adli analiz kapsamında açığa kavuşturulması sistem üzerinde bulunan uçtan uca güvenlik yapısına katkı sağlamaktadır.

Siber saldırılar içerisinde vakaların çözüm süreci uzadıkça sisteme verilen tahribat o ölçüde artmaktadır. Bu nedenle yönetimli müdahale ürünleri veya sistemden elde edilen veriler kullanılarak yapılan hızlı incelemelerin ve tespitlerin büyük önemde önüne geçen bir yapıdır. İncelemeler sonucunda elde edilen belli göstergeleri, tespit yazılımları parametreleri kontrol ederek tüm sistem üzerinde detaylı gösterge değerleri tespit edilir, Linux sistemler üzerinde adli vakalar üzerinde inceleme yöntemlerinin nasıl olduğu ve sistemde kalıcılık bırakmaya çalışan göstergeler tespit edilerek analiz süreçlerinin aktarılması amaçlanmıştır

Bu tez çalışmasının tamamlanmasında yardımlarını esirgemeyen danışmanım Sayın Doç. Dr. Fatih ERTAM'a, Fırat Üniversitesi Adli Bilişim Mühendisliğinde görevli hocalarıma ve desteğini esirgemeyen aileme teşekkür ederim.

Büşra AYTEKİN
ELAZIĞ, 2022

İÇİNDEKİLER

Sayfa

ÖZET

Linux Sistemler için Derinlemesine Adli Analiz Yapılarak Kalıcılık Yapılarının Tespit Edilmesi

Büşra AYTEKİN

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Adli Bilişim Mühendisliği Anabilim Dalı

Temmuz 2022, Sayfa: xi + 54

Günümüzde, siber saldırganlar ele geçirdiği makineler üzerinde hızlı bir şekilde yayılım gösterebilmektedir. Olay müdahale ekipleri, saldırının izlerini tespit etmek ve olası tehditleri takip etmek için güvenlik ihlaline maruz kalan makineler üzerinde uçtan uca inceleme yapmaktadır. Olay müdahale ve adli analiz süreçlerinde dijital delillerin incelenmesi ve kovuşturma evresine geçiş yapılması büyük önem taşımaktadır. Windows işletim sistemlerinde Adli bilişim uzmanları, saldırının takibi sürdürebilmesi için bazı makinelerden toplu ve hızlı şekilde veriler toplayıp analiz edebilme imkanına sahiptir. Linux açık kaynak kodlu işletim sistemlerinde görünürlük daha kısıtlı olduğundan ilgili kaynakların değerlendirilmesi ve anlamlandırılması gerekmektedir.

Adli analiz süreçlerinin yaygınlık göstermesi ve gelişen teknoloji yapısı ile Linux açık kaynak kodlu işletim sistemlerinde de saldırının kaynağının ve yayılımın tespiti için dosya sistem kayıtları veya log dosyalarının toplanması analiz süreçleri yönetilmiştir. Windows işletim sisteminde adli delil nitelikleri daha fazla ve açık iken, Linux sistemlerde saldırı aktiviteleri görünürlüğü bakımından daha azdır. Saldırganlar belirli yöntemler ile sistemleri ihlal etmekle kalmayıp, sistem üzerinde kalıcılık bırakarak zamanlanmış görevler ekleyerek sistemden bilgi toplama amaçlı mekanizmalar üretmeye çalışmaktadır.

Adli bilişim uzmanının, vakanın hızlı analizi için canlı bir sistemden veya adli bir imaj içerisinden önemli işletim sistemi dosyalarını toplaması yeterli olacaktır. Bu tez çalışmasında, Linux işletim sistemlerinde adli analiz süreçlerinin yönetilmesi, saldırganların Linux sistemlerde kalıcı olmak için hangi yapıları kullandıkları test edilerek ve tespitler analiz süreçleri ışığında aktarılacaktır.

Linux sistemlerde kalıcı olan saldırı aktivitelerini tespit edememek kurumsal ağ için büyük tehdit oluşturmaktadır. Bu tez çalışması kapsamında, Linux işletim sistemi üzerinde yer alan cihazların aktif dizinlerinden toplanan veriler ile saldırı aktivitelerinin tespiti ve kovuşturma evresine kadar bulunan sürecin yönetilmesi ve zamanlanmış saldırı görevleri yaparak sistem üzerinde uzun yıllar kalıcı olmayı amaçlayan birtakım işlemler aktarılmıştır.

Anahtar Kelimeler: Kalıcılık Mekanizması, Adli Analiz, Olay Müdahalesi, Log İnceleme

ABSTRACT

Detection of Persistence Structures by Performing In-Depth Forensics Analysis for Linux Systems

Büşra AYTEKİN

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Digital Forensic Engineering

July 2022, Pages: xi + 54

Today, cyber attackers can spread rapidly on the machines they have seized. Incident response teams conduct an end-to-end inspection of compromised machines to detect traces of the attack and track down potential threats. In the incident response and forensic analysis processes, it is of great importance to examine digital evidence and make a transition to the prosecution phase. In Windows operating systems, forensic experts have the opportunity to collect and analyze data from some machines in a fast and collective way in order to continue the attack. Since the visibility is more limited in Linux open source operating systems, it is necessary to evaluate and make sense of the relevant resources.

With the prevalence of forensic analysis processes and the developing technology structure, file system records or collection of log files were managed in order to determine the source and spread of the attack in Linux open source operating systems. While forensic evidence features are more and clear in the Windows operating system, attack activities are less visible in Linux systems. Attackers not only violate the systems with certain methods, but also try to create mechanisms for collecting information from the system by adding scheduled tasks, leaving persistence on the system.

It will be sufficient for the forensic expert to collect important operating system files from a live system or a forensic image for rapid analysis of the case. In this thesis, the management of forensic analysis processes in Linux operating systems will be tested by testing which structures the attackers use to stay on Linux systems and the findings will be conveyed in the light of the analysis processes.

Failure to detect persistent attack activities on Linux systems poses a great threat to the corporate network. Within the scope of this thesis, some processes aiming to be permanent on the system for many years by performing timed attack tasks and detecting attack activities with the data collected from the active directories of the devices on the Linux operating system and managing the process up to the prosecution phase are conveyed.

Keywords: Persistence Mechanism, Forensic Analysis, Incident Response, Log Investigation

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

Kısaltmalar

DFIR	: Digital Forensics and Incident Response
EDR	: Endpoint Detection Response
FTP	: File Transfer Protocol
HTTP	: Hyper Text Transfer Protocol
IPS	: Intrusion Prevention System
OS	: Operating System
APT	: Advanced Persistence Threat
SANS	: SANS Institute
SFTP	: SSH File Transfer Protocol
SOAR	: Security Orchestration, Automation and Response
SSH	: Secure Shell
EOE	: Evidence of Execution
SIEM	: Security Information and Event Management
IDS	: Intrusıon Detection System
RAM	: Random Access Memory

1. GİRİŞ

Olay müdahalesi ve adli analiz süreçlerinde tespit hızlı müdahale aşamaları, saldırı göstergeleri ve ilgili vakaya ait elektronik delillerin toplanması ve saklanması oldukça önem arz etmektedir. Söz konusu elektronik delillerin bütünlüğünün bozulmaması açısından kopyasının alınarak detaylı analiz edilmesi gerekmektedir. Bu birebir kopya imaj dosyasıdır. İmaj adı verilen birebir kopya mantıksal ve fiziksel olarak ayrılmaktadır. Dosya sisteminin tamamının incelendiği kopyalama fiziksel, belirli bir bölümün inceleneceği veri depolama biriminde mantıksal imaj alma yöntemine başvurulmaktadır. Olay müdahale aşamasında imaj alma türü konuya bağımlı olarak gelişmektedir. Olay müdahale süreçlerinde ortamda yer alan bütün elektronik delil niteliği taşıyan cihazlar adli kopyası alınarak incelenmelidir.

Günümüzdeki siber saldırılarla karşı kaşıya kalan kurum veya kuruluşlara ait kurumsal ağda saldırganlar hızla yayılım gösterebilmektedir. Yayılım gösteren saldırı aktivitesi ile kısa sürede birçok elektronik cihaz (Telefon, Bilgisayar, Sunucu ve hatta kamera gibi cihazlar) saldırganlar tarafından ele geçirilebilir. DFIR ekipleri, söz konusu vakanın yaşandığı ortamda saldırının kaynağı ve yayılımın tespiti için ele geçirilen cihazlardan elektronik delil toplamakta ve incelemektedir. Gelişmiş teknolojilerde uç nokta tehdit tespit ürünleri (EDR) aracılığı ile binlerce sensör aynı anda takip edilebilmektedir. Bu delil kaynaklarını, gizli dosyaları araştırarak bilgi toplamak, herhangi bir araştırma için son derece yararlı olabilir [1]. Temel olarak, dijital adli soruşturma süreçleri, bulguları incelemek, analiz etmek ve ilgili paydaşlara sunmak için kanıtların tanımlanması, toplanması ve elde edilmesini içerir [2]. İlgili kaynaklar ve loglarının toplanması birtakım güvenlik ürünleri üzerinden takip edilmesi şeklinde ilerletilmektedir Elektronik delil toplarken, ilgili sistemlerin çalışmasının devam ettirilmesine veya hizmet kesintisi sağlamamasına dikkat edilmesi gerekmektedir. Bu sebeple, adli bilişim uzmanı siber saldırılardan etkilenen sunucu veya bilgisayarlardan canlı olarak elektronik delil elde etmelidir. Saldırganlar tarafından erişilmiş olan cihazlardan saldırının kaynağının ve yayılımın tespiti için Linux işletim sistemine sahip sistemlerde birkaç dosya sistem kaydı veya log dosyalarının toplanması ile sağlanabilir. Adli bilişim uzmanının, vakanın hızlı analizi için canlı bir sistemden veya adli bir imaj içerisinden önemli işletim sistemi dosyalarını toplaması yeterli olacaktır. Bu sayede fiziksel veya mantıksal disk görüntüsünü analiz etmek için saatler harcanmadan, ilgili vakanın çözülmesi sağlanabilir.

1.1. Tezin Amacı

Bu tez çalışmasının 5 temel amacı bulunmaktadır.

- Olay müdahale yönetim süreçlerinin çerçevelerini aktarmak

- Derin analiz yöntemleri ile tehdit tespiti yöntemlerini aktarmak
- Sistem üzerinde saldırganların bıraktığı kalıcılık mekanizması yöntemlerini aktarmak
- Açık kaynak kodlu yazılımlar kullanılarak adli delil inceleme ve kovuşturma süreçlerini aktarmak.
- Gelişmiş Kalıcılık Mekanizması değerlerini sistem üzerinde tarama metotları kullanarak belirlemek ve çıktıları anlamlandırmak.

1.2. Bulgular

Bu tez çalışmasında öncelikle adli delil elde etme ve olası olay süreçlerinde müdahale aşamaları aktarılarak Linux sistemler üzerinde adli delil elde etme yöntemleri ve araçları kullanılarak yapılan testler ile detaylı bir şekilde çalışmalar yapılmıştır. Kalıcılık bırakma yöntemleri aktarılarak saldırganların iz bırakma yöntemleri test edilmiştir.

Mevcut kaynaklar ile delil elde etme yöntemleri, temel delil dizinleri, log kaynakları, zararlı yazılım tespitleri ve diğer tüm olay kavuşturma süreçlerinde kullanılması gereken yöntemler belirlenmiştir.

5 adet senaryo üzerinden saldırı yöntemleri belirlenmiş ve aşamaları raporlanmıştır.

1.3. Tezin Organizasyonu

Bu tez çalışması 7 bölümden oluşmaktadır. Tez çalışmasının ikinci bölümünde olay müdahale süreçlerinden bahsedilerek, Linux işletim sistemlerinde adli analiz, derin analiz ve kalıcılık mekanizmalarından bahsedilerek 3 ana başlık halinde ele alınmıştır. Bu başlıklar da ise mevcutta bulunan bazı siber güvenlik çözümlerine değinilip yapılmış olan büyük saldırıları ve saldırıya uğrayan sistemlerden adli delil elde etme yöntemleri üzerinde durulmuştur.

Tez çalışmasının dördüncü bölümünde siber istihbarattan bahsedilerek 3 ana başlık altında ele alınmıştır. Beşinci bölümde ise materyal ve metot 6 ana başlık altında ele alınmıştır. Bu başlıklarda kalıcılık mekanizmaları senaryoları ve tespit yöntemleri ele alınarak geliştirilmiş olan tarama yöntemlerine yer verilmiş ve tespit sonuçları raporlanmıştır. Altıncı bölümde ise bulgular ve tartışma alanına yer verilmiştir. Tezin yedinci ve son olan bölümünde ise sonuç ve önerilerden bahsedilmiştir.

2. OLAY MÜDAHALE SÜREÇLERİ

Olay müdahalesi, siber güvenlik vakasına bütün olarak müdahale etmeyi amaçlar. Güvenlik olaylarına sistematik bir şekilde yaklaşmak ve başarılı bir şekilde süreç yönetimi sağlamak amaçlanmaktadır. Olay müdahalesi ve olay müdahale döngüsü, siber saldırı durumunda aktiveyi hızla kontrol altına almak, zararı en aza indirmek ve olaydan deneyimler elde edilerek yeni önlemlerin alınması için adımlar atılmasıdır. Olay müdahalesi, şüpheli bir siber saldırı ihlaline hazırlanmak, tespit etmek, kontrol altına almak ve ortadan kaldırmak için bir kuruluş tarafından sorumluluk alınan bir yapıdır. Süreç yönetiminde tespit aşamasından ortamın iyileşmesine kadar geçen süreç takip edilmektedir. Bir olay müdahale planında, siber saldırılara karşı önleme yapılmasının yanı sıra sistemin verilerini korumak, itibarını ve maddi hasar kayıplarını da korumayı amaçlamaktadır. Enfekte olan cihazlardan saldırının kaynağının ve yayılımın tespiti için işletim sistemi üzerinde sistemlerden birkaç dosya sistem kaydı veya log dosyalarının toplanması ile sağlanabilir. Adli bilişim uzmanının, vakanın hızlı analizi için canlı bir sistemden veya adli bir imaj içerisinden önemli işletim sistemi dosyalarını toplaması yeterli olacaktır. Bu sayede fiziksel veya mantıksal disk görüntüsünü analiz etmek için saatler harcanmadan, ilgili vakanın çözülmesi sağlanabilir.

Olay müdahalesinde, bir ortamda siber saldırılardan etkilenen yüzlerce cihaz olabilir. Söz konusu cihazlar üzerinde anlık veriler elde edilmesi veya ön bilgi olarak adlandırdığımız triyaj verisi toplanılması yeterli olacaktır. Linux sistemler üzerinde ilgili kayıtların toplu halde elde edilebilmesi için birçok hazır araç kullanılmaktadır. Linux sistemde dosya dizin yapısı ve gerekli EOE(Evidence of Execution) değerlerinin toplanması için standartlar mevcuttur. Toplanan kayıtlar ile vakanın analiz süresi ve analiz yapan kişilerin iş yükü azaltılmaktadır. Bu tez çalışmasında Linux işletim sistemine sahip cihazlardan ve dosya sistem kaydının içerisinden log dosyalarının elde edilmesi yöntemlerine ve ilgili vakanın kök nedeninin tespit edilmesi için analiz edilmesi gereken kayıtlardan veri elde edilmesi hususunda detaylı olarak çalışmalar yapılmıştır.

Linux işletim sistemlerinde güvenliğin sağlanması yapılacak sıkılaştırma süreçlerinin gerçekleştirilmesi için yapılan konfigürasyonlar sonucunda saldırı parametrelerine karşı önlem seviyesini artırmak olay müdahale süreçlerinin önemli bir parçasını oluşturmaktadır.

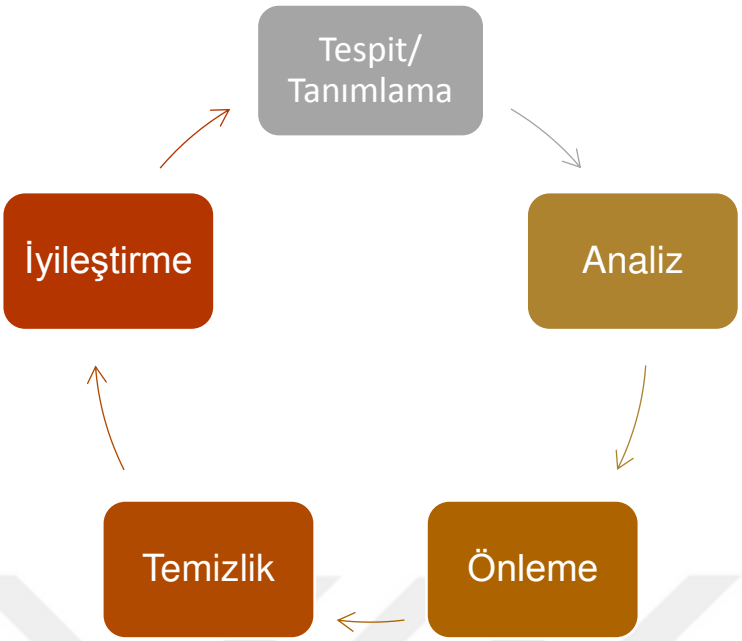
Kurum ve kuruluşlar özelinde SOAR gibi güvenlik ürünleri, siber güvenlik operasyonlarının otomatikleştirmesini sağlayarak sistem üzerinde hızlı aksiyon alınarak hızlı çözüm ve hızlı aksiyon süreçleri yönetilebilir. Güvenlik analistleri diğer güvenlik ürünleri ile entegrasyon yapılmış ilgili sistemlerde süreçleri otomatikleştirilmesi sonucunda tek bir ürün üzerinden anormal durum tespit ederek analizini yapmak ve iyileştirme aksiyonlarını çıkartabilmektedir.

Günümüzde adli bilişim süreçlerinde, kurumsal bir olay müdahale prosedürleri giderek daha fazla kullanılmaktadır. Hazırlık kapsamında, bir kuruluşun olay müdahale sürecini hızlandırmak için bir siber saldırının öncesinde alabileceği prosedürler olarak tanımlanır. İlgili prosedürler üzerinde yer alan tanımlamaların girdilerini kapsamaktadır. Güvenlik ürünlerinin planlanması ve süreç içerisinde yönetimi büyük önem taşımaktadır. Olay müdahalesinde zaman kısıtlıdır ve dijital kanıtların hızlı bir şekilde toplanmasını ve analiz edilmesini gerektirmektedir. Mevcut olabilecek güvenlik ihlaline müdahale edilirken, adli bilişim açısından sağlam kanıtların edinilmesi, saldırgan tehdidinin hızla kesintiye uğraması veya etkisiz hale getirilmesi, ortaya çıkan ekonomik ve itibar kaybın en aza indirilmesi ile dengelenmelidir [3]. Olay müdahalesinde amaç siber saldırıların detaylı şekilde tespitini gerçekleştirmek ve bu saldırılara olabildiğince zamanında etkili olarak müdahale etmektir. Saldırı etkilerini en aza indirgemek ve sistemde bütünsel bir iyileştirme sağlamak amaçlanmaktadır. Sistemler üzerinde sağlanan iyileşmenin yanı sıra saldırı vektörlerinin sistem üzerinden tamamen silinmesi, saldırganın tespit edilmemiş dosya ve dizinlerde kalıcılık oluşturması, zamanlanmış görev oluşturması amaçlanmaktadır.

Dijital adli sonuçlarda yeterli güveni sağlamak için çeşitli yöntemler geliştirilmiştir [4]. Farklı koşullar altında veri çıkarmak için özel adli teknikler ve beceriler gerekmektedir [5].

Siber saldırı ve tehdit yönetim süreçlerinde belirli politika ve prosedürlerin takip edilmesi güvenlik sıkılaştırmalarının sistem üzerinde önemli seviyelerde tutulması kurum ve kuruluş veri güvenliği, bütünlüğü açısından önem taşımaktadır.

Siber saldırılara karşı, yönetilebilir bir olay müdahale döngüsü; hazırlık, tespit etme ve analiz, temizlik ve kurtarma, saldırı sonrası alınacak önlemler olarak üzere dört aşamadan oluşmaktadır. Olay müdahalesi süreçlerine ait döngü NIST tarafından belirlenmiştir [6]. Olay müdahalesi süreçleri Şekil 2.1'de yer almaktadır.



Şekil 2.1. Olay müdahale döngüsü

2.1. Tespit Tanımlama

Linux sistemlerde Adli Analiz işlemlerinde tespit ve tanımlama aşamaları saldırı aktivitelerinde görünürlük sağlamanın temelini oluşturmaktadır. Siber saldırıdan etkilenen yapının ağ ortamının tanınması, bu tehditlerin belirlenip sistem üzerinde oluşturduğu riskleri belirlemek gerekmektedir. Saldırıya uğramış sistemin ağ ortamında konumu, üzerinde çalışan uygulamaların varlığı, bulunduğu topoloji gereği riskleri, sistemin internete açık olma durumlarının araştırılması gerekmektedir.

Sistem üzerinde bulunan saldırı aktiviteleri, kullanıcı taraflı anormal aktivitelerin tespiti ve tespit edilen olaylarının uygun bir şekilde sınıflandırmak için kritik, yüksek, orta veya düşük önem dereceleri belirlenmektedir. Ayrıca hızlı bir şekilde harekete geçebilir ve kolluk kuvvetlerinin siber olayları detaylı ve aktif olarak araştırması ve ele almasına yardımcı olabilir [7].

Aynı zamanda büyük kurumlarda görev ve yetkilendirme talepleri belirli çerçevelerde olduğundan tespit edilen anormal durum hususunda alınan aksiyonlar ve görev yapılandırmaları büyük önem taşımaktadır. Anormal durumun tespiti ve tanımlama aşamasında elde edilmesi gereken verilerin tespiti kaynakların tahsis edilmesi ve planlamanın düzgün şekilde ilerlemesine imkan sağlar.

Güvenlik ürünleri üzerinde oluşturulan kurallar, saldırı tabanlı oluşturulmaktadır ve analistler tarafından kontrolleri sağlanmaktadır. İlgili anormal durumların tespiti sistem üzerinde oluşması ve alarm türlerine göre tespitinin yapılması önem taşımaktadır.

Kurumsal ağ ortamındaki kötü niyetli aktivelerin tespiti için güvenlik kontrollerinin sağlanması bütünüdür. Ağ üzerindeki aktivelerin takibi için IDS ve IPS alarmların takibi, kural yazımı ve alarmları oluşturulabilir. IDS ve IPS yapıları kurum güvenliği açısından büyük önem taşımaktadır. IDS (Intrusion Detection System) saldırıları tespit etmeyi amaçlarken IPS (Intrusion Prevention System) sistemleri saldırıyı durdurma, önleme üzerine kurgulanmıştır. Kurumsal ağda bulunan bütün uç noktaların izlenmesi, güvenlik ürünlerinin ajanların kurumları yapılması ile makineler üzerinde, hesap çalma, yayılım, zafiyetlerin sömürülmesi gibi kötücül aktivitelerin tespiti sağlanmalıdır.

Kurum içerisinde tehdit istihbarat servislerinin aktif olarak kullanılması, araştırmacı kaynaklar, derin internet gibi alanlar detaylı incelenmelidir. Bu gibi alanlardan alınan bilgilerin incelenmesi, çalınan kurumsal bilgilerin izlenmesi, tespit edilmesi ve ihlal bildiriminin yapılması KVKK (Kişisel Verilerin Korunması Kanunu) açısından da büyük önem taşımaktadır. Kurum içerisinde entegre çalışılan kuruluşların güvenliği kurulan bağlantılar açık portlar, güvenlik duvarı yapılandırmaları gibi durumlar için kontroller ve konfigürasyonlar tam yapılmalı, dış güvenlik ürünlerinde tespit edilen zararlı parametreler tüm kurum içerisinde aratılmalıdır. İyi eğitimli ekiplerin, doğru olay müdahale planlarına uyum sağlaması, ekiplerin kötü niyetli aktiviteyi tespit ettiğinde, uygun bir şekilde öncelik tanıyabilmesi ve daha geniş organizasyonları nasıl duyurularda bulunacaklarını yönetmeleri gerekmektedir.

Kurum içerisinde son kullanıcı tarafından da birtakım bildirim yapılandırmalarının bulunması büyük önem taşımaktadır. Son kullanıcılar ihlal tespiti yaptığında güvenlik ekiplerine bildirimde bulunabilmelidir.

Uygun yöntemler tespit edildikten sonra yapılan tüm iyileştirme ve çalışmalar sistem üzerinde kurumsal ağı korumaya yönelik olmalıdır. Aktivelerin izlenmesinde görevli olan ekiplerin, herhangi bir siber saldırı olayının tespitinde acele karar vermemeli, uygun önlemler alınmalıdır [8].

Vakanın kök sebebinin bulunmasında sistemin ne olduğu alınacak önlemler konusunda büyük önem taşımaktadır. Güvenlik ürünleri üzerinde bir son kullanıcı ürünü üzerinde oluşan zararlı yazılım tespiti yapmışsa alınan önlem ile kritik bir sunucu üzerinde yapılan işlemler sonucu alınan bir alarmda alınması gereken aksiyon çok daha farklı olmak zorundadır. Tespit yapılan sistemde önemli olan sistem veya servis üzerinde çalışan uygulamaların ne amaçla kullanıldığı, sistemde firewall üzerinde açık portların bulunup bulunmadığına dair bilgilerin açığa kavuşması tespit aşamasında büyük önem taşımaktadır.

2.2. Analiz

Tespit edilen anormal durumun bulunduğu sistemin uçtan uca analiz edilmesi gerekmektedir. Linux işletim sistemlerinde adli analiz aşaması detaylı olarak yapılmalıdır.

Windows işletim sistemlerinde dosya sistemi kayıtları, erişim logları kayıtları, antivirüs logları kayıtları, registry kayıtları gibi delil analizleri bulunmaktadır.

Analiz aşamasına başlamadan önce hazırlık süreçleri yönetilmektedir. Hazırlık aşamasında, analizcilerin yaygın olarak kullanılan ve erişilebilen alanların analizi yapılmaktadır. En yaygın siber saldırı olayları veya sistemlerinize doğrudan etki edecek riskleri belirleyerek hazırlık süreçlerini bu şekilde yönetebiliriz. Söz konusu risklere müdahale edilmesi durumda operasyonel olarak rehberlik edecek ve eyleme geçirilebilir durumda olan senaryo adımları oluşturulmalıdır.

Linux açık kaynak kodlu işletim sistemlerde adli delil analizi yapılırken sistemde bulunan öncelikli zafiyetlerin tespit edilebilmesi gerekmektedir. Tespit tanımlama aşamasında sistem hakkında detaylı bilgi toplanmak zorundadır. Sistemin bulunduğu durum konum ve sistem üzerinde çalışan uygulamaların görevleri doğru şekilde bilinmeli ve analiz bütünsel açıdan izlenmelidir.

Linux sistemlerde dosya dizin yapısının incelenmesi, başarılı giriş denemeleri, başarısız girişler, son aktiviteler, çalıştırılan son komutlar, eklenen zamanlanmış görevler, log dosyaları gibi konu özelinde incelenecek alanlar ile konu açığa kavuşturulmaktadır.

Analiz süreçleri başlarken oluşan tehdidin seviyesi ve türüne göre ön kayıt alınır, ön kayıtlar herhangi bir alan ile ilgili olabilir. Ön kayıtlar sonucunda sorunun kök nedenine gidilmesi amaçlanır. Konuların bütünlüğe kavuşması için bazen ön kayıtlar yeterli olmak ile birlikte bazen uçtan uça imaj kaydı alınarak tüm dosya ve dizin bölümleri incelenir. Linux sistemlerde ön kayıt içerisinde ilgili konu özelinde tespit edilen zararlıya yönelik ilgili dosyaların çekilerek, zaman kaybı olmadan incelemeye başlanması şeklinde olmaktadır.

Sistem üzerinde dosya sistem kayıtları, oturum açan kullanıcılar, yetki yüksekliği bulunan dosyalar, başarılı ve başarısız girişler ve daha birçok delil kaynağı incelenir. İnceleme sonucunda elde edilen bulgular ışığında önleyici veya iyileştirici faaliyetler yapılmaktadır.

Analiz yapılırken bütünsel açıdan bakılarak zararlı parametrelerin sistem üzerinde zamanlanmış görev veya kalıcı hasar bırakmamasına yönelik analiz çalışmaları dahil edilmelidir. Linux sistemlerde uçtan uca imaj alınabilmesi ve detaylı inceleme yapılabilmesi için açık kaynak kodlu araçlar mevcuttur. İlgili yazılımlar aracılığı ile sistemde uçtan uca inceleme yapma imkanı bulunmaktadır

2.3. Önleme

Siber saldırı sonucunda oluşan kötücül aktivite izlerinin tespit edilmesi bazı durumlarda analiz aşamasında iken kurumsal ağ üzerinde gerekli engelleme ve izolasyon işlemlerinin yapılması gerekmektedir, saldırının tekrar yaşanmaması için önlemlerin alınması sağlanmalıdır.

Analiz aşaması bazen 24 saat, bazen ise günler alabilmektedir. Bu süreçte elde edilen dosyaların imza bilgisin zararlı olduğu tespit edilirse, anlık olarak önleme işlemleri yapılmalıdır.

Kurum genelinde dosya ismi, hash bilgisi, domain adresi veya istek yapan zararlı adreslerin engellenmesi işlemleri saldırının önlenmesi konusunda büyük önem taşımaktadır.

Saldırının yayılımını engellemek için gerekirse anlık önlemler alınması gerekmektedir. SIEM, EDR gibi güvenlik ürünleri ile tüm kurum genelinde önlemler alınmaktadır.

Bir olay tespit edildikten veya tanımlandıktan sonra analiz bulgularının sonucunda elde edilen veriler ile uygulamaya geçirilen bölümdür. Önleme aşamasının temel amacı hasarı kontrol etmek ve daha fazla hasar oluşmasını engellenmektir. Önleme aşamasında SANS ve NIST gibi standart işlemlerin bulunduğu platformlardan tavsiye ettiği tüm adımlar uygulanmalıdır. SANS adli bilişim konularında uluslararası araştırmalar yapan bir örgüttür. Özellikle "olay müdahalesi için daha sonra ihtiyaç duyulabilecek herhangi bir kanıtın imha edilmesini önlemek için" engellemeler yapılmalıdır.

Saldırı vektörleri tespit edilen Linux sistemler üzerinde zararlının silinmesi, zararlı–sürecin durdurulması konsol üzerinden yapılmaktadır. Güvenlik ürünü bulunan sistemler üzerinde güvenlik ajanlarının sağlık durumunun kontrol edilmesi ve güvenlik ajanı bulunmayan ortamların öncelikli olarak kurulum aşamalarının tamamlanması gerekmektedir.

2.4. Temizlik

Siber saldırı sonucunda oluşan kötücül aktivite izlerinin kurumsal ağ üzerinde temizlenmesi, yok edilmesi ve saldırının tekrar yaşanmaması için yeniden kurulumların yapılması gerekmektedir.

Bu aşamada sistem üzerinde yapılan testler büyük önem taşımaktadır. Sistemin tamamen temiz olduğundan veya zararlıların sistem üzerinde herhangi bir dizinde bulunmaya devam etmediğinden emin olunmalıdır.

Yeniden kurulum talebinde bulunduğumuz sistem yöneticileri yedekleme dosyalarından sistem kurulumunu yapmış olma ihtimaline karşı, sistemi zararlı yönde etkileyen işlemi yedekleme dosyalarından tekrar kurumsal ağ içerisine eklemiş olabilirler. Enfekte sistemin temizliğinin kontrol edilmesi bu açıdan büyük önem taşımaktadır.

2.5. İyileştirme

Kurtarma aşaması ile olayı geride bırakıp, kuruluşun itibarı ve ekonomik kayıplarını önlemek için gelecekte benzer siber saldırı olaylarla mücadele hazırlıklı olunması gerekmektedir. Siber saldırının kök nedeninin anlaşılması, iyileştirmelerin uygulanması ve geri bildirimlerin sağlanması gibi döngüden oluşmaktadır [9]. Her olaydan deneyim elde edilmesi ve bazı olay müdahale dokümanlarının güncellenmesi sağlanmalıdır. Siber güvenlik dünyasında; son 3 yıl içerisinde %20 artış olarak, uç nokta güvenlik çözümü pazarı gelirlerinin öneminin artacağı

olacağı tahmin edilmektedir [10]. Güncel kaynaklar ve raporlamalar sonucunda elde edilen veriler ile sistemleri etkileyebilecek tehditler takip edilerek hızlı cevap alınması gerekmektedir.

Sonuç olarak, SOAR, EDR, IPS, IDS gibi güvenlik sistemlerinde uygun alarmların oluşturulması ve sistemlerin yeni kurallar aracılığı ile yetkin bir şekilde izlenmesi sağlanmalıdır.

Sistemde bulunan kural tanımlamaları aracılığı ile anormal durumların tespit edilmesi sağlanmalıdır. Düzenli şekilde kural tanımlamaları kontrol edilerek yanlış pozitif (false positive) alarm durumları açısında sıkılaştırma çalışmaları yapılmalıdır.

3. LİNUX İŞLETİM SİSTEMLERİNDE ADLİ ANALİZ

Olay müdahale çalışmaları kapsamında işletim sistemine göre yönetilebilirlik büyük önem taşımaktadır. Adli analiz işlemlerinde analistler, dijital kanıtların kullanımında mevcut durum ve gelişen eğilimlerle ilgili sonuçlarını formüle ederler [11]. Güvenlik topluluğu kötü niyetli kişilerle otuz yılı aşkın süredir savaşmakta ve kötü amaçlı yazılım süreçlerini tespit etmek için çalışmaktadır [12]. Dijital veri biçimleri artık birçok suç eyleminin soruşturulmasında ve suçlanmasında rol oynasa da, bu kanıt türü için tasarlanmış herhangi bir inceleme yönteminin etkililiğini engelleyebilecek araçların ve süreçlerin kullanımına ilişkin artan endişeler vardır [13]. Sonuçta ortaya çıkan herhangi bir yorumun güvenilir olması için dijital olayların yeniden yapılandırılması, iddia edilen herhangi bir suçta kullanılan ortamla uyumlu olması gerekmektedir [13][14].

Gelişen teknoloji dünyasında, günlük hayatta teknoloji ile iç içe oluşumuz dolayısıyla her türlü elektronik alet ve cihazdan adli analiz işlemleri mümkün olmaktadır. Salgın hastalıklar gibi güncel olaylar sırasında video konferans uygulamaları ana iletişim yöntemi olmaya devam ettiğinden, bu sistemler tarafından üretilen adli delilleri anlamamız ve analiz etmemiz önemlidir [15]. Dosya sistemleri dijital adli soruşturmalar sırasında hayati bir rol oynar ve bu şekilde toplanan adli kanıtlar yasal işlemler için büyük önem taşır [16]. Delillerin orijinal durumda olmasının bozulması konunun kovuşturma evresine gelmesini engellemektedir ve bu saldırganlar delilleri yok ederek, izlerini silerek sistemde kalıcı olmaya çalışmayı amaçlamaktadır [17]. Anti-adli bilişim kavramı, adli delil sürecini bozma ve edinme, analizi ve / veya kabul edilebilirliği engelleme gibi durumlara sebebiyet vermektedir [18] .

İşletim sistemi özelinde adli analiz işlemlerinin yanı sıra teknolojik cihazlar ve ürünler özelinde dahil adli analiz işlemleri mümkündür. Modern akıllı telefonlarda, sistem performansları çeşitli temel alt sistemlerle sıkı sıkıya ilişkilidir.

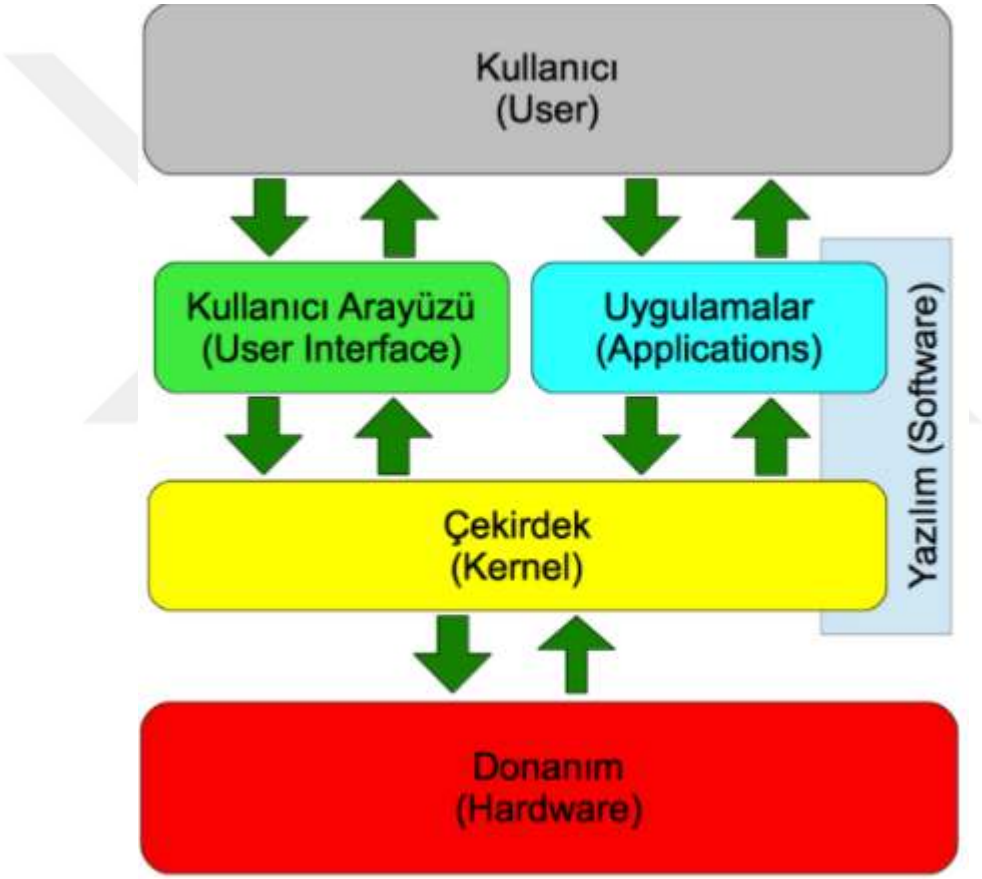
Özellikle, yıllar içinde dahili depolama çok önemli hale geldi çünkü sistemle ilgili içeriğe erişmek için yoğun bir şekilde kullanıldı [19]. Veri kümesi, saldırı tespitinin analizi için siber güvenlik araştırmalarının çeşitli alanlarında kullanılabilir, saldırı senaryosu yeniden yapılandırması ve saldırı göstergeleri oluşturulabilir [20].

Linux işletim sistemleri, kendi üzerinde kurulu güvenlik özelliklerine sahiptir ve kullanıcıların kendilerini kötü amaçlı yazılımlara karşı korumalarına yardımcı olma potansiyeline sahiptir. Bununla birlikte, Linux işletim sisteminin de saldırganlara karşı bağışıklığı yoktur [21].

3.1. Linux İşletim Sistemi Yapısı

Linux işletim sistemi yüklendiği cihazda kontrol sağlayan bir yazılımdır. İşletim sistemi yapısını bilmek, cihazların bir sisteme bağlı oldukları ve bağlı oldukları sistemde kullanılan geçmiş olayları ve etkinlikleri yeniden yapılandırmaya yardımcı olur.

Kernel, bir linux işletim sisteminin ana bileşenidir ve bir bilgisayarın donanımı ile ilgili süreçleri yönetir. Shell ise kullanıcı ile bir işletim sistemi çekirdeği arasında bir arayüz sağlayan bir programdır. Bir işletim sistemi için kernel ve shell en önemli temel iki bileşendir. İşletim sisteminde iki temel bileşenle beraber başka programlar da bulunur. Programlar, dosya sistemi ve komutlar. Şekil 3.1'de işletim sistemi yapısı belirtilmiştir. [22].



Şekil 3.1. İşletim sistemi yapısı

Dosya Sistemi, genellikle işletim sisteminin altında bulunan ve verilerinizin depolama alanı üzerindeki konumunu yöneten bir katmandır. Farklı koşullar altında veri çıkarmak için özel adli teknikler ve beceriler gerekmektedir [13]. Linux dosya sistemine gömülü FTP veya HTTP sunucusu ile erişilebilir [23].

Bir dosya sisteminin yapısı işletim sisteminin verimi ve hızını etkilemektedir. Linux dosya sistemi türleri aşağıda verildiği gibidir:

Ext: Extended dosya sistemi, sanal dizinde depolanan dosyalar hakkında bilgi veren inode sistemi kullanır. İnode sistemi, sanal dizin içerisinde depolanan dosyalar hakkında iz olarak adlandırılan yol bilgisi veren bir alan içerir. Dosya bilgisini saklamak için her bir fiziksel aygıt üzerinde ayrı bir inode tablosu oluşturulur. Sanal dizinde depolanan her dosyanın inode tablosunda bir girişi vardır. Her dosyada izlenen aşağıda veriler nedeniyle dosya sisteminin adına Extended denilmiştir.

- Dosya adı
- Dosya boyutu
- Dosyanın sahibi
- Dosyanın ait olduğu grup
- Dosya için erişim izinleri

Linux, inode tablosundaki her bir inode, dosya sistemi tarafından veri dosyaları yaratmakla görevlendirilmiş özgün bir inode numarası kullanılarak işaretlenir. Dosya sistemi, bir dosyayı belirlemek inode numarasını kullanır.

Ext2: Ext dosya sisteminin temel yeteneklerinin genişletilmiş hâlidir. Ext2 dosya sistemi, sistemdeki her bir dosya hakkındaki inode tablo biçimini iz ek bilgisine genişletir.

Ext3: Günlük dosyasına sadece inode bilgisini yazar ve veri blokları depolama aygıtına başarılı bir biçimde yazılana değin bu bilgiyi silmez. Ext3 dosya sisteminde kullanılan günlükleme yöntemi, komut satırı işlemi ile dosya sistemi oluştururken veri ya da geri yazma kiplerinden birine değiştirilebilir.

Ext4: Ext3 dosya sisteminin genişletilmiş halidir.

Btrfs: Disk yapılandırma ve disk üzerinden özet alma imkanı sağlar, Oracle tarafından geliştirilmiştir. Performans olarak çok güçlüdür.

JFS: JFS dosya sistemi, düzenli günlükleme yöntemini kullanır, günlüğe sadece inode tablosu verisini depolar, güncel dosya verisi depolama aygıtına yazılıncaya dek kaldırmaz. JFS dosya sistemi depolama aygıtına yazılan her bir dosya için bir grup blok ayırarak depolama aygıtında daha az parçalanmaya neden olur. IBM tarafından yapılan eski dosya sistemidir.

XFS: Eski dosya sistemidir ve küçük dosyalarla yavaş çalışır. XFS dosya sistemi geri yazma kipi günlüklemeyi kullanır, güncel veri günlükleme dosyasına kaydedilmediği için bazı riskler taşır.

Linux sistemlerde günlükleme (journaling) özelliği, bilgisayar üzerinde yapılan işlemlerin loglarının başka bir yerde tutulmasını sağlar. Bu özellik sayesinde yapılan son işlemlere ulaşılabilir. Herhangi bir sistem çökmesi durumunda, sistemde yapılan son işlemlere ulaşılıp bu işlemlerin tekrarlanmasıyla verilerin kaybedilmemesi sağlanır. Saldırganlar ilgili sistemlerden elde ettikleri bilgileri yedekledikten sonra sisteme zarar verebilirler. Linux işletim sisteminde kullanılan en kararlı ve sağlam günlükleme sistemi XFS dosya sistemidir. Günlükleme

seçeneklerinden metadata günlükleme özelliğinde ise, sadece sistemde yapılan değişiklikleri, günlük içerisinde metadata adı verilen dosyaların içerisinde saklar.

Linux/Unıx dosya sistemine dosya eklemek için yapılması gereken üç adım şöyledir:

- Dosyanın bulunduğu düğümün (inode) içerisindeki dosyanın büyüklüğünü arttırmak
- Dosyanın ekleneceği alanda olabilecek genişleme için yer ayırmak
- Eklenecek dosyanın, yeni ayrılmış alana yazılması

Metadata günlükleme olayında, bu üçüncü basamak loglarda tutulmaz. Eğer üçüncü basamak gerçekleşmeyip birinci ve ikinci basamak kurtarma işlemi sırasında tekrarlanırsa, dosya çöplüğe atılır.

3.1.1. Linux İşletim Sistemlerinde Kullanıcı ve Grup Yönetimi Yapılandırması

Linux işletim sistemleri üzerinde çalışan uygulamaların birçoğu, sistemle etkileşime geçmek ve işlemleri yürütmek için kullanıcılar oluştururlar. Örneğin Oracle Veritabanı sunucusunun "oracle" adında bir kullanıcısı mevcuttur. Sistemde oluşturulan her bir kullanıcı adıyla birlikte birde, bu kullanıcı adına uygun grup oluşturulur. Linux işletim sisteminde varsayılan ayar olarak kullanıcılar kendi isimlerine uygun gruplara üye yapılırlar. Çeşitli görevleri yerine getirmek için kullanıcılardan bağımsız gruplar da oluşturulabilir. Kullanıcılar burada bulunan yetkilendirme durumlarını ihlal ederek sistemlere girmeye çalışmaktadır. Saldırganlar yetki fazlalığı bulunan grupları hedef almaktadır.

Kimin hangi bilgilere erişeceğini kontrol edebilmek kritiktir, güvenlik kontrolü ve hatta yasal bir gereklilik olabilir. Kullanıcı hesaplarının sınırlandırılmasını korur bilgilenir ve aynı zamanda sistemin kendisini hem kötülükten hem de basitçe korur hatalar [24].

Bir bilgisayar sisteminin kırılmasında izlenen yolların büyük çoğunluğu, makine üzerinde geçerli bir kullanıcı hesabına sahip olunmasından geçer. Güvenlik açıklarından faydalanmayı amaçlayan kötü niyetli kişiler bu sunucu üzerinde bulunan hesaplardan bir tanesini eline geçirdiğinde işi büyük ölçüde kolaylaşmaktadır. Bu nedenle ana makine üzerindeki bütün şifrelerin en az root kullanıcının şifresi kadar iyi korunması gereklidir. Minimum karakter sayısı güncel yayınlanan değerlere göre 12 olmalı ve 42 gün içerisinde değişim yapılmak zorundadır.

Linux işletim sistemde kullanılan şifrelerin genel özelliklerini kısıtlamak mümkündür. Bunun için "/etc/login.defs" dosyasında minimum password değerini güncellemek yeterli olacaktır.

Kullanıcı parolalarının düzenli olarak değiştirilmesi ve PAM gibi çözümlerle sağlanabilir.

Parolaları boş olan kullanıcılar ortamdan kaldırılmalıdır.

3.1.2. Kullanıcı Yönetimi Etcpasswd Yapısı

Bir cihaz farklı kişiler tarafından kullanıldığı durumlarda, kullanıcılar arasında ayrım yapmak gereklidir. Kişiye özel işlemlerin gerekli dizinler içinde depolanması ve ayrıştırılması uygun olmaktadır. Sonuçta, her kullanıcı için farklı bir kullanıcı ismi verilir ve herkes sisteme bağlanmak için kendi ismini kullanır. Aynı zamanda birçok kullanıcının yetkilerinin topluca belirlenmesi gerektiğinde grup hesapları kullanılmaktadır. Gruplar, kendisine dâhil olan kullanıcıların gruba verilen haklardan yararlanmasını sağlar. Grup yetkilendirmeleri kendi grup yapısında önemlidir. Grup hesapları aynı zamanda kullanıcı hesapları gibi dosya ve dizinlere erişim ve sistem ayarlarının yapılabilmesi için gerekli tanımlamalara olanak sağlar.

Kullanıcıların birden fazla gruba üye olmaları mümkündür. Böylelikle birkaç grubun haklarından yararlanabilirler. groups komutu kullanılarak, etkin kullanıcının hangi gruplara üye olduğu görülebilir. Unix / Linux sistemlerde kullanıcı veri tabanı **"passwd"** dosyasında bulunur. Linux işletim sistemleri üzerinde pek çok ön tanımlı kullanıcı gelir. Ancak bunlardan sadece **"root"** kullanıcısı sisteme interaktif shell bağlantısı kurabilir. Bu da Unix sistem yöneticilerinin eskiden beri uyguladığı geçersiz öntanımlı shell ayarı ile sağlanır.

Kullanıcı yönetimi için kullanılan komutlar **"useradd"**, **"usermod"** ve **"userdel"** dir. Bu komutlar **"/etc/passwd"** dosyasında girdiler oluşturur ve bu girdileri düzenler. **"passwd"** ve **"shadow"** dosyaları hakkında ayrıntılı açıklamayı yazımızın devamında bulabileceksiniz.

"/etc/passwd" dosyasında tanımlı ön tanımlı shell uygulamalarını inceleyebiliyoruz. Sanal sistemlerde, Grep, normal bir ifadeyle eşleşen satırlar üzerinde düz metin aramak için kullanılır. Parametre olarak "**:0:"** kullanılır.

Bir saldırganın saldırı gerçekleştirmek üzere herhangi bir geçici kullanıcı oluşturup oluşturmadığını belirlemek için **"find / -nouser -print"** komutu kullanılarak oluşturulan kullanıcılar listelenir.

Donanımda bulunan CPU yani merkezi işlem birimi, ya da kısaca işlemci, RAM yani bellek ve diğer disk, network aygıtı gibi çevresel aygıtları yönetir.

3.1.3. Linux İşletim Sistemlerinde Temel Delil Dizinleri

/etc: Konfigürasyonların tutulduğu ana dizindir. Her bir uygulama için konfigürasyonlar ayrı klasörde tutulur. Windows işletim sistemlerinde karşılığı olarak **SYSTEM**, **SAM**, **SECURITY** dosyaların tutulduğu **C:\Windows\System32\config** dizinine karşılık olmaktadır.

/var/log: İşletim sistemi için birincil loglama dizinidir. Uygulama ve sistem logları saklanır. Windows karşılığı **C:\Windows\System32\Winevt\logs** olarak düşünülebilir.

/home/$USER: Kullanıcı verisi ve kullanıcıya özel konfigürasyonların saklandığı dizindir. Windows'daki **%userprofile%** olarak düşünülebilir. Root kullanıcısı için **/root** dizinidir.

Cihaz üzerinde çalışan anormal servisleri görüntülemek için **"service –status -all"** komutu kullanılmaktadır.

Sisteminizdeki büyük boyutlu dosyalar sistem güvenliği açısından büyük rol oynamaktadır ve bunların izinlerini vermek dosyalar üzerinde yetkilendirmeler yapmak, hedefleriyle birlikte tanımlamalarını girmek gerekmektedir. Büyük boyutlu dosyalar sisteme brute force saldırı etkisi yaratmaktadır. **"find /home/ -type f -size +512k -exec ls -lh {} \;"** komutu ile sistemde oluşan büyük boyutlu dosyalar tanımlanabilmektedir.

Bir olay müdahale sürecinde sistemde mevcut olan anormal bir dosyayı görüntülemek için **"find / -mtime -2 –ls"**

$PATH, işletim sistemi üzerinde kabuğa yürütülebilir dosya için hangi dizinleri arayacağını söyleyen bir dizin listesi görüntüler. Dosyalar ve ilgili dosyanın bulunduğu dizin bilgisinin elde edilmesi için "**echo $PATH"** komutu kullanılmaktadır.

Tablo 3.1'de Linux sistemlerde bulunan adli analiz işlemlerinde kullanılabilecek temel delil dizinleri gösterilmiştir.

Tablo 3.1. Linux sistemlerde temel delil dizinleri

Delil Dizini	**Tespit Alanı**
cat /etc/resolv.conf	Domain Name Server adreslerini gösterir.
cat /etc/hosts	Host tanımları mevcuttur. Buradaki tanımlar resolv.conf içerisinden daha detaylıdır.
cat /etc/shadow	Parola hash'leri tutulur.
cat /etc/group	Grup üyelikleri listelenir.
cat /etc/sudoers	Yönetici haklı kullanıcıları gösterir.

/proc dizini; süreç kontrollerini ve diğer sistem bilgilerini tutan dosya sistemi. Bu dosya sistemi disk üzerinde yer kaplamaz, tüm dosyalar çekirdeğin bir uzantısı şeklinde tutulmaktadır. Proc temel delil dizini altında elde edilebilecek bilgiler Tablo 3.2'de sunulmuştur.

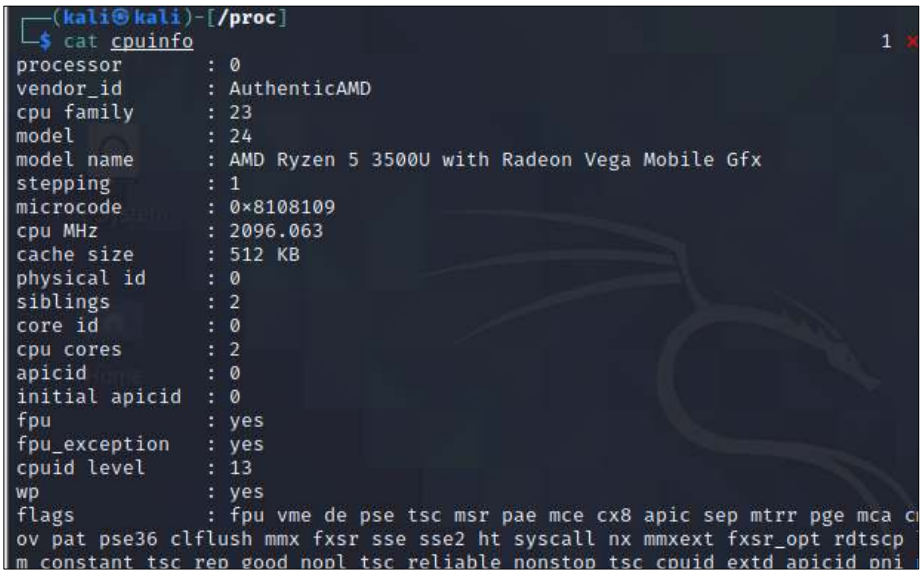
Tablo 3.2. /proc dizini bilgisi

Delil	**Kontrol Alanı**
Devices	Hazırda çalışan çekirdek içinde desteği bulunan aygıt sürücülerini listeler.
Dma	Hangi **DMA** kanallarının kullanıldığını belirtir.
Filesystems	Hazırda çalışan çekirdek içinde desteği bulunan dosya sistemlerini listeler.
Ports	Halen hangi giriş/çıkış iskelelerinin kullanıldığını belirtir.
Kcore	Sistem hafızasının görüntüsü
Cpuinfo	İşlemci modeli, tipi ve performansını bildirir.

/proc/mounts dosyasını olay müdahale sorumlusu olarak, cihazda bilinmeyen bir ekleme olup olmadığını kontrol etmek için cihaz üzerinde bulunan mevcut olan ve **var/log** dizini altında bulunan dosyaları **"cat /proc/mounts"** dizini içerisinde tespit edebiliriz.

/proc/iomem: Fiziksel adreslerin cihazların belleğiyle eşleştirilmesini içerir.

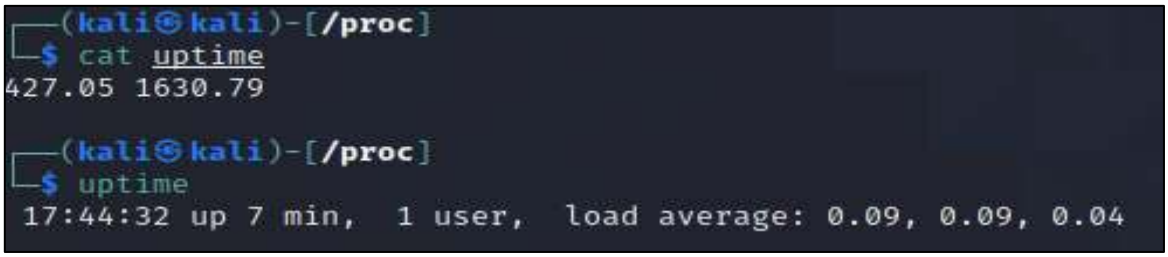
/boot/system.map ve **proc/kallsyms;** bu iki dosya adli depolama için önemlidir, çünkü bunlar tüm global değişkenlerin adreslerini ve o anda çalışan çekirdeğin dışa aktarılan yöntemlerini içerir. İşletim sistemi hakkında bilgi elde etmek için **"cat cpuinfo"** komutunu kullanılabilir. Şekil 3.2'de bu duruma örnek gösterilmiştir. İşletim sisteminde kaç işlemci olduğu, işletim sistemi modeli, cpu leveli, cpu core değerleri gibi alanlar belirlenmektedir. Adli delillerde işletim sisteminin özellikleri ile tehdit türünün eşleşmiş olması gerekmektedir.



Şekil 3.2. CPU bilgisi

Saldırgan izlerini takip etmek amacıyla İşletim sistemi hakkında işletim sisteminin ne zamandan beri açık olduğuna dair saniye cinsinden değer verebilir. Aynı zamanda ikinci seçenek

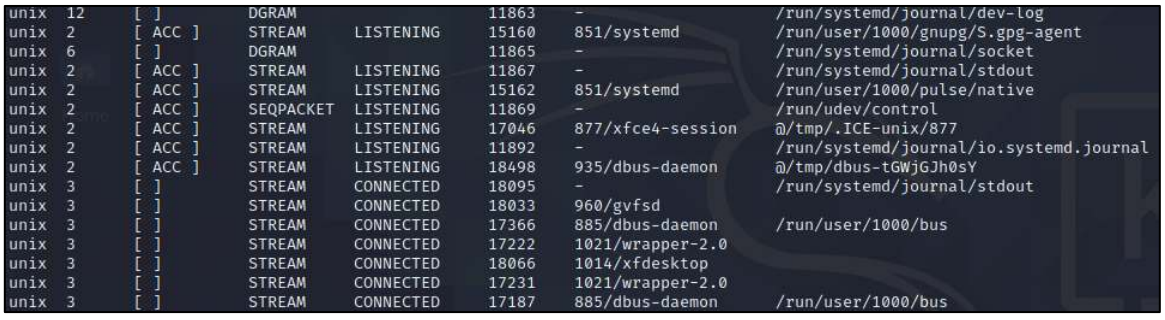
olarak tarih bazında bilgi elde edilebilir. Her iki seçenek için ekran görüntüsü Şekil 3.3'de verilmiştir.



Şekil 3.3. İşletim sistemi bilgileri

Linux platformunda canlı hafıza analizi yapılırken, bellekteki yapı düzeni bilgilerinin kesin bilgisini gerektirir, genellikle derleme zamanında oluşturulan sembollerin hata ayıklamasıyla elde edilir [26]. Her bir adli delili görüntüleyebilmek için ayrı bir dosya incelenebilir, Linux sistemde her bir dosya sisteminin ve dizin yapısının içerisinde adli artifact değerleri bulunmaktadır. Sistem üzerine takılan USB bellekleri görüntülemek için örnek olarak aşağıda gösterildiği gibi bir işlem yapılır. Saldırganlar USB bellek aracılığı ile sisteme kalıcılık bırakarak, cihaz her açıldığında saldırganın bilgi toplaması gerekli alanlardan bilgi toplanması işlemleri devam etmektedir. "İfconfig –a" komutu ile sisteme entegre cihazların listesi elde edilebilir.

Söz konusu saldırgan tarafından etki altına alınmış makine ile başka hangi makineler iletişim kurmaktadır, sistemde şüpheli ağ bağlantılarının analiz edilmesi, makine internete açık bir ortamda bulunuyor ise detaylı analiz edilmesi, makineye yapılan şüpheli bir dinleme ve tarama aktiviteleri bulunuyor mu detaylı analiz edilmesi gerekmektedir. Başarılı, başarısız paket detayları dizin bilgileri gibi bilgiler Şekil 3.4'de gösterilen çıktıda bulunduğu gibidir.



Şekil 3.4. Şüpheli bağlantıların incelenmesi

3.1.4. Linux Sistemlerde Log Dosyaları

Linux sistemlerde log dosyaları oluşan saldırı aktivitesinin açığa kavuşturulması konusunda büyük önem taşımaktadır. Adli incelemelerde sistem üzerinde bulunan erişim logları

kaynak parametreleri, kalıcı görev düzenlemeleri, user ve grup logları, kaynak parametreleri, kullanıcı geçmiş logları, güvenlik logları ve parametreleri, error logları, adli incelemeler yapılırken sistemde yapılan giriş tarihleri çok önemlidir. Sonuç olarak sistemde adli analiz yapılabilmesi amacıyla log dosyaları 4 ana başlık içerisinde değerlendirilmektedir. Uygulama Logları, Olay logları, Sistem logları ve Servis loglarıdır.

Kullanıcı oturum bilgileri, mail sunucuları kalıcılık mekanizmaları, giriş denemeleri gibi bilgiler Linux işletim sisteminde sistem içerisinde alınan loglama yapısının kullanılması ve kaynak bilgilerinin detaylı olarak elde edilmesi sonucunda bulunmaktadır.

Sisteme yapılan giriş denemeleri, yetkisiz kullanıcı tarafından yapılan girişler gibi konular tespit edildiğinde, sistemde önleyici çalışmalar anlık olarak ilerletilmektedir. Linux sistemlerin tutmuş olduğu **wtmp** ve **btmp** dosyaları ile bu bilgiler elde edilebilir.

Wtmp: Giriş yapılan zaman bilgisi ve hangi kullanıcıdan giriş yapıldığı tarih ve saat bilgisi ile verilir.

Btmp: Dosyası ile en son ne zaman sistemde başarısız giriş yapıldığı tarih ve saat bilgisi ile verilir.

Web üzerinden erişim logları, error logları, mail logları gibi dosyalar ve içeriğinde bulunan bilgiler adli bilişim çalışmaları kapsamında değerlendirilerek nihai sonuç ve sorunun kök sebebi elde edilmektedir. Log dosyalarının anlamlandırılarak raporlama yapılması ve saldırgan takibinin yapılması ve olası tehditlerin açığa çıkarılması konusunda elzemdir.

Linux sistemlerde log dosyaları **var/log** dizini altında bulunur. Tablo 3.3' de Log dosyalarının görevi görüntülenmiştir.

Tablo 3.3. Linux sistemlerde log dosyaları ve içerdiği bilgiler

Log Dosyası	**Görevi**
messages	Sistem başlangıcı/ sistem logları tutar.
lastlog	Son kullanıcı girişlerini ve zaman bilgisini tutar
cron	Zamanlanmış görevlere ait tüm log bilgisini tutar.
secure	Kimlik doğrulama yetkiler ve güvenlik ile alakalı tüm logların tutulduğu alandır.
Dmesg	Bilgisayar açıldığı andan itibaren çekirdek dosyaların yazıldığı bir yapı.
maillog	Sistem üzerinde çalışan mail sunucusuna ait loglar yer alır.
Syslog	İşletim sistemi hatalarını ve uyarılarını takip eder.
Auth.log	Başarısız oturum girişleri kullanıcı yetkilendirme mekanizmaları

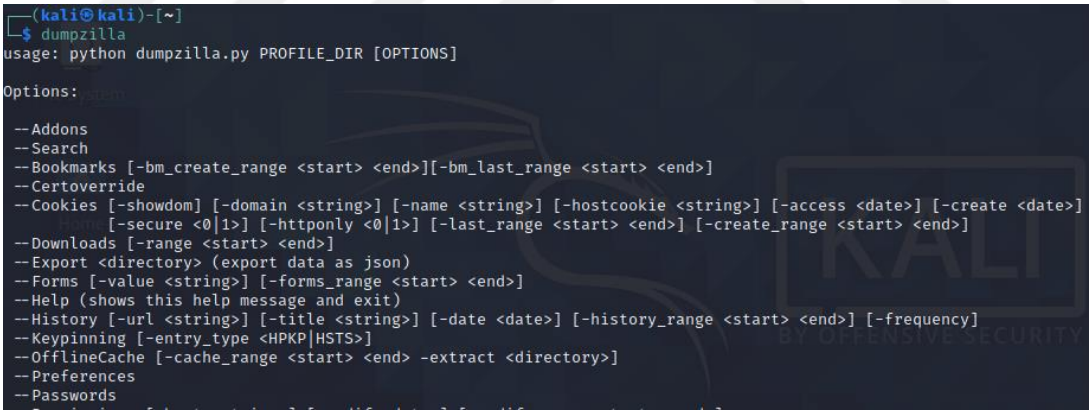
3.1.5. Linux Sistemlerde Tarayıcı Kayıtları

Web tarayıcı kullanarak ön bilgi edinme ya da olaya ait iz bırakan alanlardan ön araştırma yapılması her işletim sisteminde büyük öneme sahiptir. Linux işletim sistemlerinde de tarayıcı analizi yapılarak detaylı bilgi elde edilebilir. Tablo 3.4' de tarayıcı analizinde ilgili adli delillerin, lokasyonları bulunmaktadır.

Tablo 3.4. Linux sistemlerde tarayıcı geçmişi tanımlamaları

Tarayıcı	Delil Dizini
Firefox	/home/$USER/.mozilla/firefox/*.default
Chrome	/home/.config/chromium/Default

Suçlunun hangi tarihte hangi URL adresine erişmek istediği ve giriş yaptığı bilgisi elde edilerek ve bununla birlikte çerez bilgilerini bulundurmaktadır. Aşağıda gösterildiği gibi Linux sistemler üzerinde yer alan bazı araçlar ile (**dumpzilla**) tarayıcı üzerinde kayıtlı şifreler, etiketler, indirilenler, tarayıcı geçmişleri gibi bilgiler elde edilebilir. Şekil 3.5'de detayları gösterildiği gibi Dumpzilla aracı ile tarayıcı izleri aracılığı ile saldırgan aktivitelerinin tespit edilmesi ve analiz edilmesi sonucunda işe yarar bilgiler elde edilebilir.



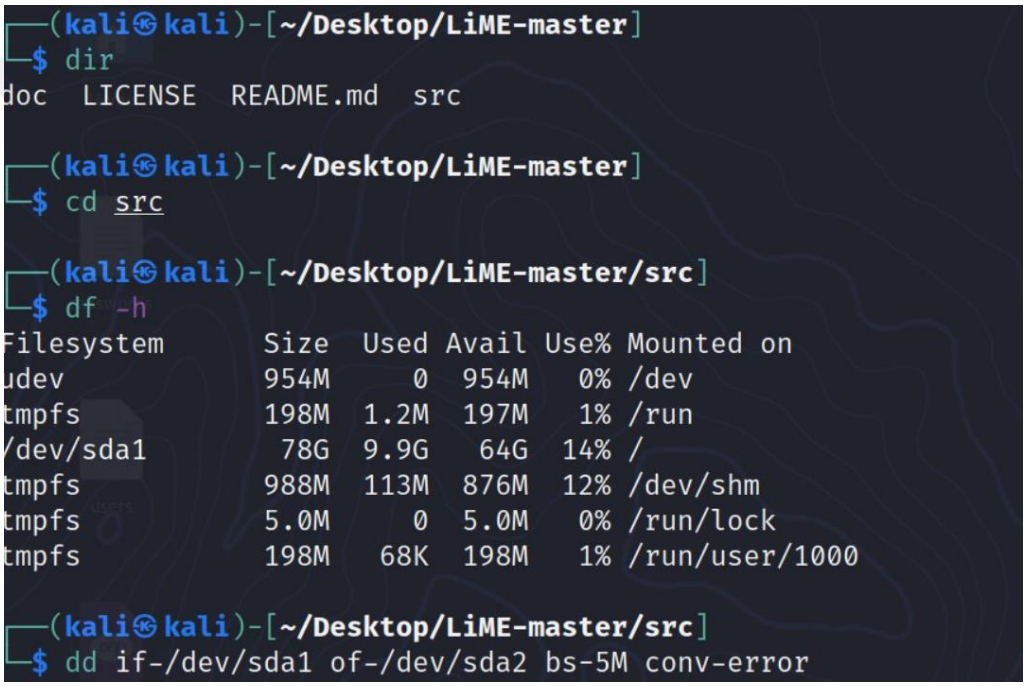
Şekil 3.5. Dumpzilla aracı ile elde edilebilecek bilgiler

Örnek olarak saldırgan sisteme erişmiş ve zararlı yazılım indirmiş, birtakım zararlı yazılımlar kullanarak sisteme zarar vermeyi yedekleme yapmayı dosya transfer etmeyi hedeflemiş olabilir. Olası tüm senaryoların değerlendirilmesinde fayda bulunmaktadır [25].

3.1.6. Linux Memory (RAM) Forensics

Ram geçici bellektir ve içerisinde kritik bilgiler barındırır. Canlı bir sistemden ram kopyasının alınması oldukça önemlidir çünkü saldırganının kaydedilmemiş dosyaları bu alanda yer alabilir. Tarayıcı bilgileri açık ağ bağlantıları, parola bilgileri sosyal medya kalıntıları gibi işlemler Ram bellek içerisinde bulunan alanlarda depolanabilir.

Diskin ne kadarının aktif olduğunu **"cat meminfo"** komutu ile **proc** dizininden elde edebiliriz. Diskte yeteri kadar alan varsa **FMEM, LİME, dd** ve **d3dd** gibi araçlar ile Linux sistemlerden hafıza analizi yapılabilir. **LIME** uygulaması ile Ram imajı alınma aşaması için örnek görüntü Şekil 3.6' da verilmiştir.



Şekil 3.6. LIME ile RAM analizi

RAM imajının alınması için **"dd if-/dev/sda1 of-/dev/sda2 bs-5M conv-noerror"** komutu ile yapılmaktadır.

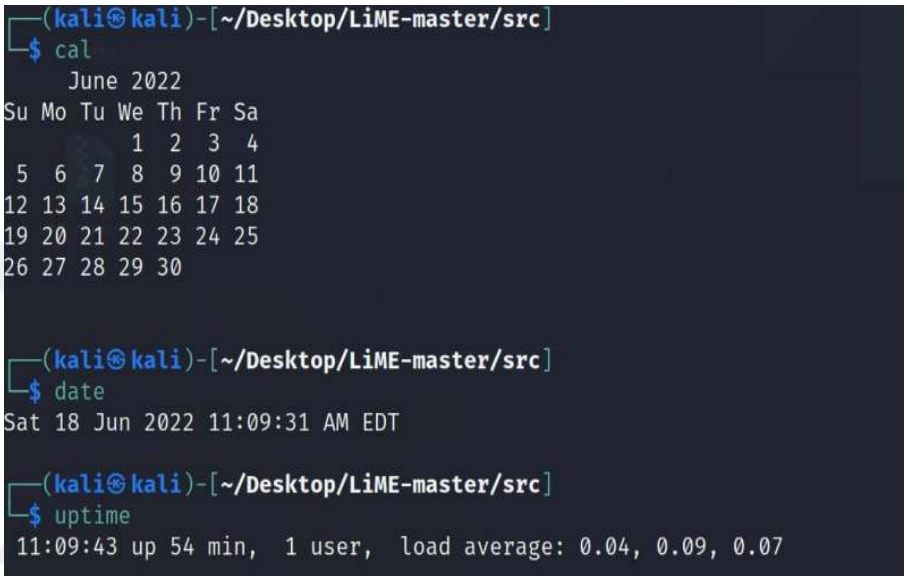
Aynı zamanda Volatilite gibi araçlar mevcut bellek üzerinde dosya sistemlerine, her analiz görevi için yalnızca işletim sistemi türünü desteklemek üzere tasarlanmış zorluklar sunar [26].

Müdahale edilen canlı sistemler ile ram analizi, ram boyutlarının artmış olması adli incelemelerde ram üzerinde tutulan bilgilerin çok önemli değer taşıması ile ram üzerinden adli vaka incelemenin önemi giderek artmıştır. Ram geçici bir bellektir. Sistem kapatılınca bilgiler uçar bu nedenle kaydedilmemiş dosyalar, sosyal medya kalıntıları, tarayıcı kalıntıları arka planda çalışan süreçler ve parola bilgileri gibi süreçleri elde etmek amacıyla RAM imajı büyük önem taşımaktadır.

4. LİNUX SİSTEMLERDE DERİN ANALİZ İŞLEMLERİ

4.1. Zaman Bilgisi

Enfekte sistemin analiz edilmeye başlaması durumunda öncelikle analist için önemli zaman dilimi tarih bilgisidir. Şekil 4.1'de gösterildiği gibi tarih bilgisi, bilgisayarın en son ne zaman açıldığı konusu gibi bilgiler analist için yol gösterici ipucu bilgiler taşımaktadır.



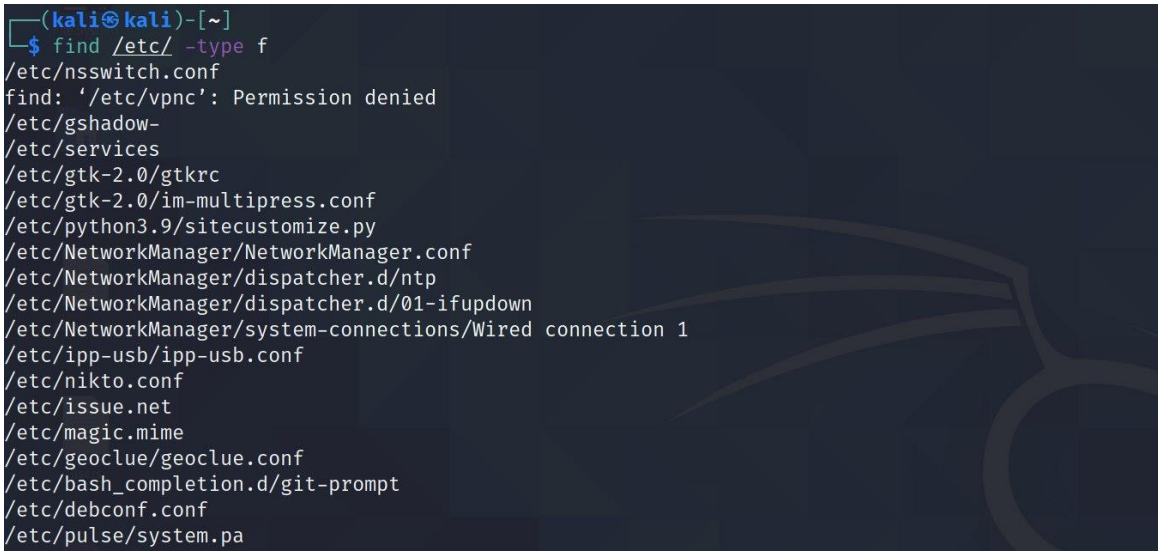
Şekil 4.1. Memory imajı alınması

4.2. İşletim Sistemi Linux Çekirdek Bilgisi

Enfekte olan sistemin işletim sistemi çekirdek yapısı üzerinde kullanılacak güvenlik ajan programlarının kurulmasını etkilemenin yanında incelenen sistemin en son ne zaman kurulduğu bilgisini tarihsel olarak taşımaktadır. Bu tarih işletim sisteminin ilgili zararlı aktiviteyle alakalı güncel olup olmaması veya zararlı dosyanın sistemin kurulumundan önce bir tarihte işletim sistemi üzerinde bulunması gibi detaylar DFIR analistine önemli bir bilgi taşımaktadır. Uname -a komutu ile "Linux siftworkstation 5.4.0-77-generic #86-Ubuntu SMP Thu Jun 17 02:35:03 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux" gibi işletim sistemi bilgilerinin detaylı bilgi elde edilebilir.

4.3. Dosya Bütünlüğü (Hash Bilgisi)

Enfekte olduğu düşünülen sistem üzerinde detaylı incelemeler yapılması adına sistemde bulunan tüm dosyalar düzenlenir. İlgili dosyaların hash değerleri gerekli kaynaklardan araştırılarak sistemde anormal durum tespiti yapılabilir. Hash özeti değişmez ve dosyanın benzersiz bir özet değerini oluşturur. Sistem üzerinde bulunan dosya ve dizinlerin takip edilmesi, kalıcı bulunan saldırı parametrelerinin kontrol edilmesi açısından kritik önem taşımaktadır. **"find /etc/ type f"** komutu çalıştırılabilir. Şekil 4.2'de dizin altında bulunan dosyalar belirlenmiştir. İlgili dosya ve dizinler kontrol edilerek şüpheli dizin ve dosyalar detaylı olarak incelenmelidir.



Şekil 4.2. Şüpheli dizin içerisinde bulunan dizinleri görüntüleme

Dosya dizinlerde hash bilgisi, özellikle canlı analiz yapılırken tespit edilmektedir. Canlı sistem üzerinden imaj alınmayacaksa sistem üzerinde şüpheli bulunan dosyaların hash değerleri tespit edilerek tehdit istihbarat servislerinden (Virüs Total, Abuse IP) araştırılır zararlı dosya hakkında detaylı bilgi elde edilir. Şüpheli dosya ve dizinlerde bulunan dosyaların hash değerlerini tespit etmek amacıyla Tablo 4.1'de belirtilen komutlar kullanılmaktadır.

Tablo 4.1. Şüpheli dosyaların Hash bilgilerinin tespiti

Komut	AMAÇ
find /etc type f | xargs md5sum | head	Dosyanın MD5 hash değerini tespit etmek.
find /etc type f | xargs sha256sum | head	Dosyanın SHA256 hash değerini tespit etmek.
hfind –i <indeks_tipi> <hash_veritabanı_dosyası>	Verilen indeks tipine göre hash tespiti yapmak.

Şekil 4.3'de dosyaların hash değerleri bulunmaktadır. Belirlenen hash değerleri tehdit istihbarat platformlarından araştırılarak zararlı yazılım tespitleri yapılmaktadır.

Şekil 4.3. Şüpheli dosyaların hash bilgisi

4.4. Olası Sızma Yöntemleri ve Giriş Noktalarının Tespiti

Analiz aşamasına başlamadan önce, sistemi hızlı şekilde gözden geçirerek saldırgan gözüyle bakmamız gerekmektedir. Linux Sistemlerde derin analiz yapılırken öncelikle kullanılan yöntemin tespitinin yapılması gerekmektedir.

Sistemin bulunduğu topolojide ağ üzerinde bulunan konumu konumu gibi değerler önem taşımaktadır. Bütünsel açıdan sisteme bakmak sistemin açıklarını tespit etmek ilgili konularda çıktıları analiz etmek önem taşımaktadır.

- Standart yollar ile sistemin bulunduğu ağ üzerinde taramalar yapılması

Linux sistemlerde açık kaynak kodlu olarak geliştirilen ve varsayılan olarak yer alan, Nmap, Nessus veya Openvas gibi sistemde tarama yaparak açıklıkları tespit etmeye yarayan araçlar kullanılmaktadır.

- Brute-force Parola Saldırıları ile Sisteme Erişilmesi

Brute Force, bir parolayı ele geçirmek için yapılan bir çeşit dijital ve kriptografi saldırısıdır. Saldırgan karakter setleri ile izleme listeleri oluşturmuş olabilir. Karakter setleri ile de bir wordlist oluşturarak sisteme deneme yapma işlemleri gerçekleştirilir. Linux sistemlerde brute force saldırıları tespiti için giriş denemeleri ve başarısız giriş denemeleri logları incelenmelidir.

Sisteme saldırgan gözüyle bakmak büyük önem taşımaktadır.

4.5. Web Uygulama Zafiyetleri Kullanılarak Sisteme Erişilmesi

Web uygulamaları üzerinde yer alan kullanıcı girdileri, HTML çıktı kodlama işlemleri, veri tabanı güvenliği, parola güvenliği gibi durumlarda yer alan zafiyetlerin sömürülmeye çalışılması ile sisteme erişmeye çalışan saldırgan profilleri mevcuttur. Enfekte sistemlerin incelenmeye başlanması aşamalarında sunucu üzerinde yer alan web servislerinin erişim logları incelenerek, şüpheli istek veya tarama gibi durumların tespiti yapılmalıdır.

Web uygulamaları üzerinde tespit edilen birçok zafiyet ve açıklık mevcuttur. Linux sistemlerde hazır araçlar sayesinde, rapıscan, skıpfish, xsspwn, gibi sistemde zafiyet ve bilgi toplanır önleme ve düzenleme aşamaları büyük önem taşımaktadır.

SQL injection, XSS, File İnclude açıklıklarından yararlanarak saldırgan aktiviteleri tespit edilmektedir.

4.6. Çalışan Servislerin Hedef Alınması

Linux işletim sisteminde anormal durumların incelenmesi ve kovuşturulması aşamalarında sistemde o anda çalışan şüpheli processlerin incelenmesi ve anında müdahale edilebilmesi büyük önem taşımaktadır. Tablo 4.2' de tespit yöntemleri belirtilmiştir.

Tablo 4.2. Çalışan şüpheli servisler ile ilgili bilgi toplanması

Komut	Görev
systemctl status <service_name>	Çalışan servisin durumu komutu listelenmektedir
systemctl stop <service_name>	Çalışan bir servis komutu ile durdurulmaktadır.
systemctl start <service_name>	Sistem tekrar başlatılırsa bildirim alınır.

Şüpheli processler tespit edilerek komut aracılığı veya sistemde var ise güvenlik ürünleri aracılığı ile toplu olarak durdurularak yayılımı engellenebilir. Çalışan processler üzerinde zararlı yazılım tespiti yapılır ise ilgili şüpheli yazılım network izole ortamında zararlı yazılım inceleme araçları ile incelenerek statik ve dinamik açıdan incelenerek zararlı yazılım yapısı ile ilgili araştırmalar, zararlının hedef aldığı sistemler belirlenmeli cihaz ve sistem üzerinde koruma çalışması tamamlanmalıdır.

4.7. Yerel ve Uzak Bağlantı Detayları

Netstat etkin TCP bağlantılarını, bilgisayarın bağlı olduğu bağlantı noktalarını, Ethernet bilgilerini, IP Routing tablosu ve gerekli iletişim kuralları üzerinden istatistikleri görüntüler. Tablo 4.3' de komut detayları verilmiştir.

Tablo 4.3. Netstat komutuna ait parametreler ve açıklamaları

Komut	Açıklama
Netstat -a	Tüm TCP ve UDP bağlantıları ekrana basar.
Netstat -e	Gelen ve giden paket sayısının istatistiklerini görüntüler.
Netstat -n	Tüm bağlantıları rakamsal olarak görüntüler.
Netstat -o	Tüm bağlantıları PID numarası ve uygulama adına göre listeler.
Netstat –p	Bağlantıların kullandığı uygulama ve PID numaralarını ekrana basar
Netstat –s	Kurallara göre istatistiksel verileri ekrana basar.
Netstat –r	IP yönlendirme tablosunun içeriğini görüntüler

Tablo 4.4'de linux sistemler için ağ bağlantıları tespit etme komutu ile paket ve protokol bilgilerinin verilmesi hususunda örnek çıktı yer almaktadır. Ağ üzerinde gönderilen paket çıktısının ağ protokolleri üzerinden detaylandırılması çıktı sonucunda verilen bilgilerin anlamlandırılması sonucunda oluşmaktadır.

Tablo 4.4. Paket trafik protokol çıktısı

```
Ip:
    Forwarding: 1
    6752 total packets received
    1 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    6749 incoming packets delivered
    3300 requests sent out
    20 outgoing packets dropped
    1 fragments received ok
    2 fragments created
Icmp:
    40 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 40
    40 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 40
IcmpMsg:
        InType3: 40
```

OutType3: 40

Tcp:

21 active connection openings

0 passive connection openings

4 failed connection attempts

0 connection resets received

0 connections established

6295 segments received

2845 segments sent out

0 segments retransmitted

0 bad segments received

4.8. Lsof Aktif Bağlantıların Listesi

Enfekte sistem içerisinde, şüpheli zaman aralıkları belirlendiğinde ilgili aktivite aralığında olay anına ve sonrasına ilişkin dosya incelemeleri yapmak, sistemde aktif olan dosya bağlantılarını tanımlamak büyük önem taşımaktadır Şekil 4.4'de sistem üzerinde bulunan aktif cihaz bilgisi tespit edilmiştir.

Şekil 4.4. Lsof aktif bağlantı görüntülenmesi

Aktif bağlantılar ve dinlenilen portlar **listen** durumundadır. Listen mod içerisinde olan bağlantılar detaylı incelenmelidir.

Lsof -Pni komutu ile analist DNS (Domain Name Server) çözümlemesi yapmadan bilgi alarak saldırgandan kendini gizleyebilir. Tablo 4.5'de komutların detayları verilmiştir.

Tablo 4.5. Lsof kullanımı

Komut	İşlev
lsof –i	Açık olan tüm network socketleri ve aktif bağlantıları listelemek için -i parametresi kullanılmaktadır.
lsof –Pni	Eğer, port ve hostname'lerin isim çözümlemesi yapılmadan numerik olarak listelenmek amacıyla kullanılmaktadır.
lsof -i :22	SSH portunu dinlemektedir.
lsof -i @IP	Spesifik bir ip adresinden açılan bağlantıları listelemek için kullanılmaktadır.

Lsof parametresi kullanıcıların açtığı dosyalar, belli bir dosyaya erişen süreçler, belli bir dizine erişen kullanıcı ve süreçler, özel bir bir sürecin açtığı dosyalar, belirli bir komut çalıştıran süreçler gibi mekanizmaların tespitinin yapılması adına Linux sistemlerde ilgili parametre kullanılmaktadır. Örnek olarak apache sunucusuna ait 18828 numaralı sürecin eriştiği tüm dosyaları listelemek isterseniz "lsof -p" parametresini kullanarak ilgili process sürecini görüntüleyebilmekteyiz.

Belirli bir komut üzerinde çalışan parametrelerin listesinin tanımlanması ve tüm süreçlerin görüntülenmesi için operasyonel süreçlerde sıklıkla kullanılır. Saldırganın çalıştırmış olduğu komutlar tespit edilerek, lsof komutu ile süreçlerini listelememiz mümkün olmaktadır.

4.9. Sistem Üzerinde Yapılan Değişiklikler

Ele geçirilmiş bir Linux sunucu üzerinde saldırganın yapmış olduğu değişiklikleri tespit etmek amacıyla son günlerde değişen veya yeni eklenen dosyalar hakkında bilgi toplanmalıdır. Sistemde bir zararlı dosya indirilip, önemli olmayan bir dizinde kullanılmış ve kendisi çalışan bir process üzerine eklenmiş olabilir. Bu durumlarda orijinal dosyayı "**find"** komutu ile bulabiliriz.

Son zamanlarda değiştirilmiş/düzenlenmiş tüm dosyaların tespitini yaparak saldırganın bıraktığı etkileri detaylıca inceleyebiliriz. **"Find /etc -type -f printf '%TY-%Tm-%Td-%TT%p\n' | sort -r"** komutu ile şüpheli dizinde değiştirilen dosyaları elde edebilir dizini ve alt dizinlerde değiştirilmiş dosyaları listelemektedir.

Linux İşletim sisteminde, son bir saat içerisinde veya son iki gün içerisinde değişen dosyaların kayıtları tespit etmek amacıyla "**find"** komutu kullanılmaktadır. Sistemde root yetkileriyle **"sudo find /etc -type f -mtime -2"** komutu kullanarak son 2 gün içerisinde değişen dosyaları görüntüleyebilmekteyiz.

4.10. Dosya İzinlerinin İncelenmesi;

Linux işletim sistemlerinde, **Chmod** komutu içerisinde dosya üzerinde change mod olarak adlandırılan bir yapıdır. Kontrol edebilmek için **chmod 777** komutu kullanılmaktadır. Amaç yazma okuma çalıştırma izni bulunan tam yetkilendirilmiş dosyaları listelemek. Herhangi bir şüpheli reputasyona(imza değerine) sahip dosyanın sistem üzerinde tam yetkilendirme ile bulunmasını engellemektir. Tablo 4.6'da Dosya izinlerinin belirlenmesi ve görüntülenmesi için kullanılabilen komutlar belirlenmiştir.

Tablo 4.6. Dosya izinlerinin belirtilmesi

Komut	Açıklama
ls -lt	Loglara ait son değiştirilme zamanı bilgisini tanımlamaktadır.
ls -lu	Logların dosyasına son erişim zamanı bilgisini tanımlamaktadır.
ls -lc	Log dosyasına erişim haklarının son değiştirilme bilgisini ve izinleri belirtir.

4.11. Sisteme yapılmış başarılı veya başarısız giriş denemeleri

Linux işletim sistemlerinde **"/var/log/auth.log"** dizini altında sisteme yapılan girişlerin bilgisine ulaşılmaktadır. Enfekte olduğu tespit edilen sisteme yapılmış giriş denemelerini kontrol ederek, yetkisiz giriş tespitleri yapılmaktadır. Linux işletim sisteminde **Last** komutunu kullanarak uzaktan sisteme giriş yapmış kullanıcıların listesini elde edebiliriz. Herhangi bir kullanıcının sisteme ne zaman ve hangi tarih aralığında girdiğini elde edebilmek için **last username** komutu kullanılmaktadır.

Sistemde yetkisi bulunmayan bir kullanıcının başarılı giriş yapması şüpheleri çekmek için yeterlidir. Kullanıcının oturumunu en son ne zaman açtığı, hangi aktivitelerde bulunduğu gibi bilgiler konsolide edilerek çözümlenebilir.

Sistemde yapılan başarısız giriş denemelerinin sıklık(istek) sayısı ve buradaki anormal durumların tespit edilmesi, büyük önem taşımaktadır.

4.12. Sistemin Yeniden Başlatılma Zamanı

Adli analizlerde en önemli hususlardan biri sistem üzerinde delil bütünlüğünün korunmasıdır. Özellikle uçucu verilerin kaybedilmesi delilin bütünlüğünü etkileyebilir. Saldırgan aktiviteyi gerçekleştirdikten sonra sistemi yeniden başlatabilir. Cihazın son yeniden başlatılma zamanını tespit ederek, analiz için veri toplanmaktadır.

4.13. Sistemde Aktif Kullanıcıları Listelemek

Sistem üzerinde bulunan aktif kullanıcıları komut **journalctl -u 'systemd-logind' –since "today" –until "tomorrow"**

Linux işletim sistemlerinde **"less /var/log/auth.log"** komutu kullanarak sistemde anlık olarak bulunan kullanıcıların loglarının incelenmesi yapılmaktadır.

Linux işletim sistemlerinde ilgili komuta W parametresi eklenmesi ile sistemde aktif olarak bulunan ağ servislerinin incelenmesi ve bunları çalıştıran kullanıcıların bilgileri tespit edilmektedir.

Netstat komutu kullanılarak ağ bağlantıları daha detaylı kontrol edilebilir.

4.14. SSH Anahtarlarının İncelenmesi

Sistemde bağlantı yapılması söz konusu olduğunda güvenli şekilde bağlantı olması, saldırganın uzak bağlantı yapabileceği port bilgilerini kapatması firewall üzerinde de ilgili yaygın hedef portların kapatılması gerekmektedir. SSH bağlantısı yapılırken kapalı anahtar ve şifreli bir yapı ile hedef sisteme giriş yapılır. SSH yani 22 portu açık sistemler saldırganlar için daha görünür sistemlerdir.

SSH (Secure Shell) Uzak bağlantı parola girişleri ile güvenli bağlantı sağlanması yerine bir açık anahtar kullanılabilir. Bu özel anahtar saldırgan tarafından çaldırılmış ve başkası tarafından kullanılıyor olabilir. Sistemde bulunan SSH logları incelenerek anomali tespiti yapılmalıdır.

Saldırgan SSH & telnet oturum açma veya sistemdeki kimlik doğrulamasını belirlemek için "/var/log/" dizinine gidebilir ve ardından şunu yazabilirsiniz. Sistemde bulunan başarısız bağlantılar

"Grep sshd.\ *Failed /var/log/auth.log | less grep sshd. *Did /var/log/auth.log | less" komutu ile tespit edilmektedir. Böylelikle defalarca zorlama yapan saldırgan giriş denemelerini tespit etmek amaçlanmaktadır.

4.15. Linux Syslog ve Auditlogların İncelenmesi

Syslog linux sistemlerde loglama yapısına verilen isimdir. Geriye dönük analiz yapabilmek ve işletim sisteminde ne gibi işlemlerin olup bittiğini öğrenmek için syslog kullanılabilir. Kurum ve kuruluşlar genelinde ilgili dosyaların kullanımı ortamda bulunan Linux cihazların log entegrasyonlarının sağlıklı çalışması ve saldırı etkisi oluşturan sistemlerin incelenmesi konusunda açık bir fayda sağlamaktadır. Sistemde ne olup bittiğini anlamak, gerekli kayıtları geriye dönük incelemek ve günlük yedekleme yapıları syslog aracılığı ile yapılması sağlanır. Daha gelişmiş versiyonu Rsylog olarak bilinmektedir.

Linux Audit sistemi işletim sistemi çekirdeği tarafından sisteminizde oluşan çağrı ve olayların hemen hepsi hakkında süreç işlemlerinin loglanmasıdır. Syslog/Rsylog loglarından farklıdır; çünkü Audit logları bazı temel değişmeyen alt yapıları mümkündür.

Linux Audit logları; Audit kernel modülü, sistem çağrılarını takip eder ve yapılandırmada takip edilmesi istenen çağrılarla ilgili olayları kaydeder. Audit sisteminden denetim raporlarını çekerek diske yazmakla görevli bileşendir. Toplanan logların görüntülenmesi ve sorgulanması için de belirli audit uygulamaları belirlenmektedir.

4.16. Linux Adli İnceleme Araçları

Linux işletim sisteminde Adli inceleme işlemleri yapılırken sistem üzerinde bulunan log kaynaklarından faydalanıldığı ve dosya/dizin bazlı tutulan bilgilerin içerisinden elde edilen bilgiler doğrultusunda detaylı analiz işlemleri yapıldığı bilgisi elde edilmiştir.

Adli analiz işlemleri yapılırken manuel bulgular dışında, hazır araçlar kullanılarak adli incelemeler detaylı olarak yapılmaktadır. Kullanılan açık kaynak kodlu araçlar ile konunun açığa kavuşması acısından doğrulamasının sağlanması ve kovuşturma evresine ulaşmasına fayda sağlayacak bilgiler elde edilmiştir. Bu araçlardan bazıları aşağıda detaylandırılmıştır. Açık kaynak kodlu yazılımların kullanılması özgürlük, güvenilirlik, açısından avantajlar sağlamaktadır.

Linux, verileri işleyebilen, metin belgelerinin, resimlerin, videoların ve yürütülebilir dosyaların veri analizini gerçekleştirebilen, bu verileri araştırmacıya ilgili verileri tanımlamaya yardımcı olacak bir biçimde sunabilen ve verileri araştırabilen çok çeşitli dijital analiz cihazlarına sahiptir. Bir kaynaktan verinin alınması ve işlenmesi sistemde yapılan işlemlerin analizleri sonucunda elde edilen bulguların işlenmesi gibi süreçleri benimsemektedir.

SIFT, ücretsiz olarak erişilebilen ve sık sık güncellenen son teknoloji açık kaynaklı araçlar kullanılarak gelişmiş olay müdahale yeteneklerinin ve derinlemesine dijital adli tıp tekniklerinin gerçekleştirilebileceğini göstermektedir.

SIFT üzerinde temel bulunan dizinler dışında olay başlangıç ve bitiş zamanları adına incelemeler yapılabilir.

Zaman çizelgesi işlemleri yalnızca bir dosya üzerinde sakladığından, dosya ile ilgili geçmişin daha iyi anlaşılmayı mümkün kılar [24].

SANS SIFT adli analiz platformu sayesinde sistem üzerinde delil elde etme, analiz ve çözümleme aşamalarında Linux, Unix, Windows işletim sistemleri özelinde adli analiz işlemleri gerçekleştirilmektedir. SANS Linux işletim sisteminde hem saldırı, hem de analiz imkanı bulunmaktadır.

SANS SIFT kuruluşu adli analiz işlemlerinde standartları belirler ve gerekli delil dizinlerini poster şeklinde tanımlamış yayınlamıştır.

Linux işletim sistemi içerisinde yaygın olarak kullanılan “dd” parametresi ve aracı çoğu Linux dağıtımında (Fedora, Ubuntu) varsayılan olarak yüklenen güçlü bir araçtır. Bir klasör, dosya veya sürücünün fiziksel imaj (birebir adli kopya) oluşturmak için ve adli analizlerin tamamlanması için kullanılır. Tablo 4.7’de gösterilmiştir.

Tablo 4.7. Linux adli analiz için kullanılan araçlar ve özellikleri

Araç	Özellik
dd	Klasör veya diskin bir bölümünün veya dosyanın imajını almak için kullanılan adli analiz aracıdır.
dc3dd	Geliştirilmiş dd sürümü
dcfldd	dd'nin farklı geliştirilmiş sürümü (bu sürümde bazı hatalar var!, başka bir sürüm de github adulau / dcfldd üzerindedir
Deft	Adli Bilişim Analizi için kullanılan Linux Dağıtım
Linux Expl0rer	Python & Flask'ta yazılan Linux uç birimi için kullanımı kolay canlı adli araç

SANS gibi platformlar sayesinde sanal ortam üzerinde hazır araçlar aracılığı ile analiz işlemleri yapılabilir [27]. Rapid Response yazılımı gibi yazılımlar vasıtasıyla sistemlere uzaktan bağlantı yapılarak adli analiz işlemi yapılabilir. [28]

4.17. Linux İşletim Sisteminde Zararlı Yazılım Tespiti ve Timeline Çıkarılması

Linux'un açık kaynak kodlu işletim sistemi, kendi bünyesinde bulunan araçlar ile zararlı yazılım analizine olanak tanımaktadır. Komut satırına bağlı kalınarak ilgili zararlı yapılar üzerinde inceleme yapılabilir ve zararlının amacı, sisteme sızmak için kullandığı yöntemler detaylı analiz ile davranış ve yapısal olarak incelenerek sisteme bıraktığı etki detaylı olarak araştırılmalıdır.

Sunucu kullanımı sayısı açısından Linux sistemler, Windows işletim sistemlerine göre daha yaygın halde olduğundan zararlı yazılımlar bu sistemleri hedef almaktadır.

Linux sunucuda tarama işlemleri yapılırken kullanıcının sistemde bulunan zararlı türlerini tespit etmek amaçlanmaktadır. Kalıcılık mekanizmalarını belirlemek, zamanlanmış görevleri elde etmek söz konusu olduğunda APT tarama yazılımları devreye girmektedir.

Lynis Linux sistemlerde bulunan ve sadece kurulum dosyası ile açılan bir yazılımdır. Sistemde dosyayı açarak Lynis audit system komutu kullanarak sistem üzerinde bulunan dosya dizin yapıları taranmaktadır. Tarama yazılımları arasında ClamAV adı verilen açık kaynak kodlu antivirüs ürünü sistemde virüs, malware ve trojan gibi kötücül amaçla kullanılan dosya tespiti yapmaktadır. Sistemde zararlı yazılım tespiti yapılabilecek bir başka araç ise Chkrootkit isimli yazılımdır.

Sistem üzerinde analiz yapılırken toplanan bulguların çıktısının düzenli elde edilmesi Timeline oluşturulması analize dair bir vaka içerisinde olayın bütünlüğünü ve olayın kök sebebini sağlayabilmek için çok önemli bir unsurdur. Analiz aşamasında sistem üzerinden alınan her bir delil ile sistemde oluşan değişiklikler bütünsel olarak incelenebilir. Timeline içerisinde vaka özelinde yer alan ve compramise (enfekte) olan sistemlerin bilgileri, zararlı yazılım bilgileri,

enfekte cihazlar, enfekte userlar gibi bilgiler tanımlanarak sistem üzerinde detaylı incelemeler yapılmalıdır.

İlgili listeler formatlı bir şekilde analistler tarafından hazırlanmalı ve vaka kök sebepleri araştırılırken geçmiş vakalar göz önünde bulundurulmalıdır.

5. MATERYAL VE METOT

Linux sistemlerde derinlemesine analiz aşamaları takip edilerek tüm dosya sistemi yapısı, log dosyaları, sistem üzerinde analiz yapılarak incelemeler yapılması ile enfekte sistemde anormal aktiviteler tespit edilmektedir. Gelişmiş Kalıcılık Mekanizmaları (APT'ler), bir bilginin ve / veya kritik altyapının gizliliğini, bütünlüğünü ve kullanılabilirliğini tehlikeye atmak olan bilgili ve becerikli düşmanlar tarafından kullanılan gizli saldırılardır [13]. Saldırganlar sisteme sızmak için yetki yükseltir, zafiyet bulgusu elde ederek sisteme yerleşir, Bu saldırıları önceki yıllarda görülenden çok daha sinsi yapan şey, karmaşıklıkları ve sosyal mühendislik ve otomatik araçlar dahil olmak üzere çoklu saldırı tekniklerinin kullanılmasıdır [29].

5.1. Başlangıç Script'leri

MITRE atak vektörleri platformlarında linux saldırı kategorileri incelendiğinde, Linux açık kaynak kodlu sistemlerde kaynak kodundan tespit edilip, sistem her açıldığında otomatik olarak çalışmasını sağlayarak sistemde kalıcı olmaya çalışır. Tablo 5.1'de görülmüştür.

Tablo 5.1. Başlangıç kalıcılık mekanizmaları

Dizin	Görev
/etc/inittab,	Hizmet başlangıç komut dosyaları
/etc/init.d,	Hizmet başlangıç komut dosyaları
/etc/rc.d,	Hizmet başlangıç komut dosyaları
/etc/init.conf,	Hizmet başlangıç komut dosyaları

5.2. Zamanlanmış görev (cronjob) dizinleri

Zamanlanmış görev komutları ayrıca linux dağıtımına göre /etc dizininde yer alan cron. hourly, cron.daily, cron.weekly, cron.monthly dizinlerine atılarak da görevler zamanlanabilir. Saldırganlar saatlik günlük haftalık ve aylık periyotlarda çalışmalar ekleyerek sistem üzerinden bilgi toplamayı amaçlamaktadır.

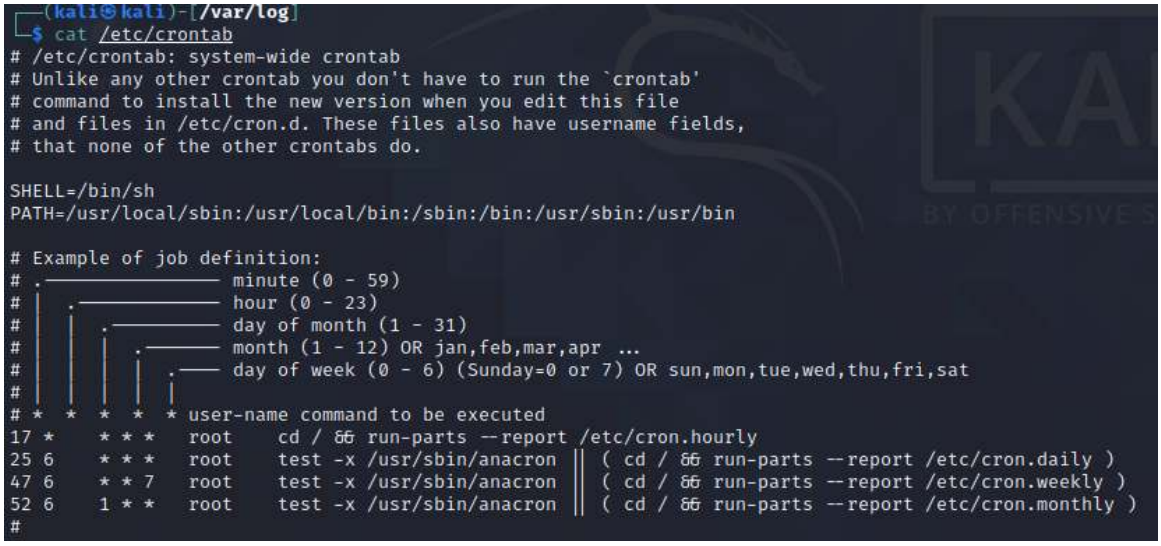
Root yetkisinde bulunan kullanıcı her ayın beşinci günü gibi özel bir zaman aralığı vererek sistemde istediği çalışmaları yapabilir. Saldırgan sistemde yetki yükseltip elde ettiği verileri sistem üzerinde düzenli periyodlarla toplayabilir.

Cron konfigürasyon dosyalarında gerekli değişiklikleri yaparak hangi kullanıcıların Cron'u kullanabileceğini hangilerine kullanım izni verileceğini belirlemek cron dizini altında yapılabilecek bir takım güvenlik ihlallerinin önüne geçmek için alınması gereken önlemlerdendir. Tablo 5.2'de örnek dizinler belirtilmiştir.

Tablo 5.2. Cron dizini kalıcılık mekanizmaları

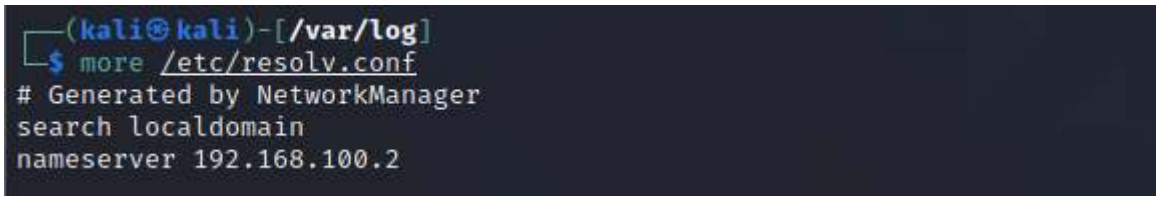
Dizin
/etc/cron*,
var/spool/cron/*

Olay sorumlusu, planlanmış şüpheli görevleri ve işleri aramalıdır. Saldırganlar zamanlanmış görevler üzerinde kalıcılık bırakarak sistemde düzenli taramalar veya tahribatlar elde edebilir. Şekil 5.1'de Crontab dizini içeri görüntülenmiştir.



Şekil 5.1. Crontab kalıcılık mekanizmaları

DNS yapılandırma sorunlarını çözmek ve aşağıdaki anahtar kelime listesinden yararlanmak için çeşitli çözümleyici bilgi türleri kullanılabilir. Şekil 5.2'de bu durum gösterilmiştir.



Şekil 5.2. Crontab kalıcılık mekanizmaları

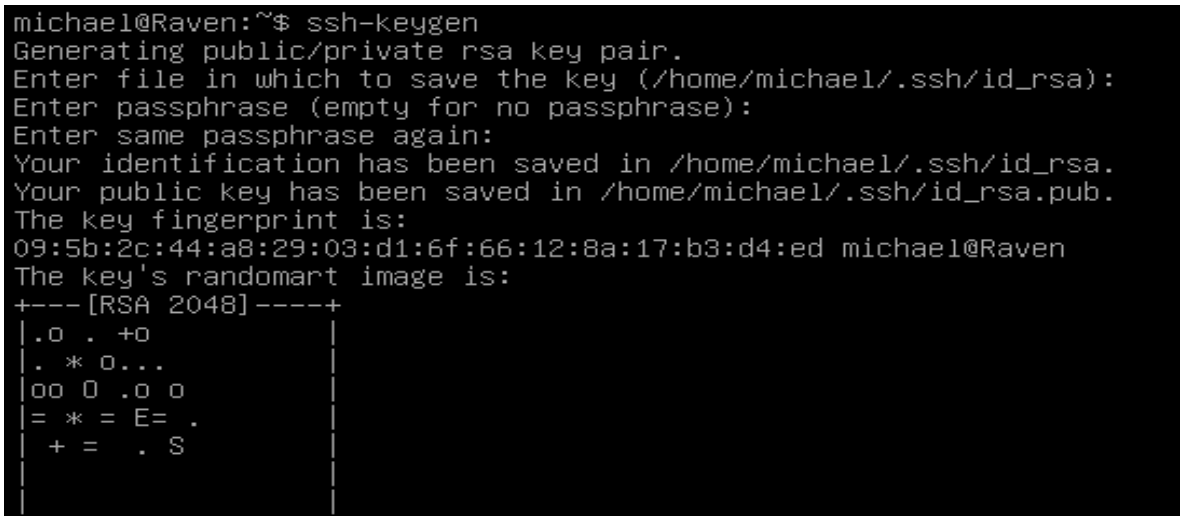
Sistem kurulum tarihine dair çok yakın bir tahmin için **/etc/ssh/ssh__host__*_key** dosyalarına bakılabilir. **$HOME/.ssh** dizininde **SSH** bağlantı detayları bulunmaktadır.

KNOWN_HOSTS, alanında bu makineden bağlanılan makineleri, **AUTHORİZED_KEYS** alanında ise bu makineye yapılan bağlantılar için public key'leri içerir. **İD_RSA** alanında ise private key'ler vardır.

5.3. SSHDOOR ile Kalıcı Arka Kapı Bırakma

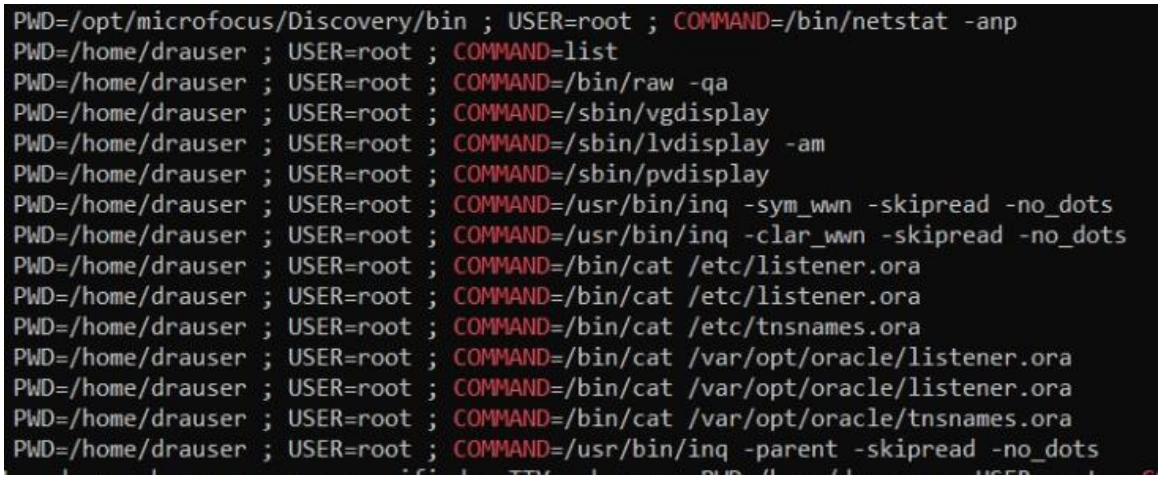
Truva atı olarak bilinen ve işletim sistemleri üzerinde backdoor bırakmayı amaçlayan zararlı dosya, SSH servisini hedef alarak elde etmeyi amaçlar. Sistemde bulunan parolaları düzenli olarak kaydetmeyi ve kimlik bilgisi hırsızının mevcut olduğunu **usr/bin/ssh** dosya, kullanıcı adını, parolayı ve hedef ana bilgisayar adını kaydeden değiştirilmiş bir yürütülebilir dosyayla değiştirerek sistemden bilgi toplamaktadır.

Authorized_Keys dosyasının incelenmesi Linux sistemlerde yetki verilmiş kalıcılık bırakan saldırganın SSH açık anahtarları **"/home/username/.ssh/authorized_keys"** dosyasından elde ederek sisteme uzak bağlantı yaparak sistemde aktif olmayı hedefleme mekanizmasına sahiptir. SSH'deki authorized_keys dosya, dosyanın yapılandırıldığı kullanıcı hesabında oturum açmak için kullanılabilecek SSH anahtarlarını belirtir . SSH anahtarlarını kullanarak **kalıcı erişimi yapılandırdığı** ve uygun yönetim gerektirdiği için oldukça önemli bir yapılandırma dosyasıdır. İlgili kalıcılık mekanizmasını sistemde oluşturmak için öncelikle ssh-keygen komut çıktısı içerisinde belirli bir anahtar çifti oluşturduktan sonra sha256 keyini authorized_keys patterni altına eklememiz gerektiği Şekil 5.3'de gösterilmiştir.



Şekil 5.3. SSHDOOR ile arka kapı oluşturma

Sistemde yapılan incelemelerde **"ssh_"** zararlısı tespit edildiğinde, secure.loglar kontrol edildiğinde linux sistem üzerinde ssh ile çalıştırılan komutlar Şekil 5.4' de verilmiştir.



Şekil 5.4. Root yetkisi ile çalışan komutlar

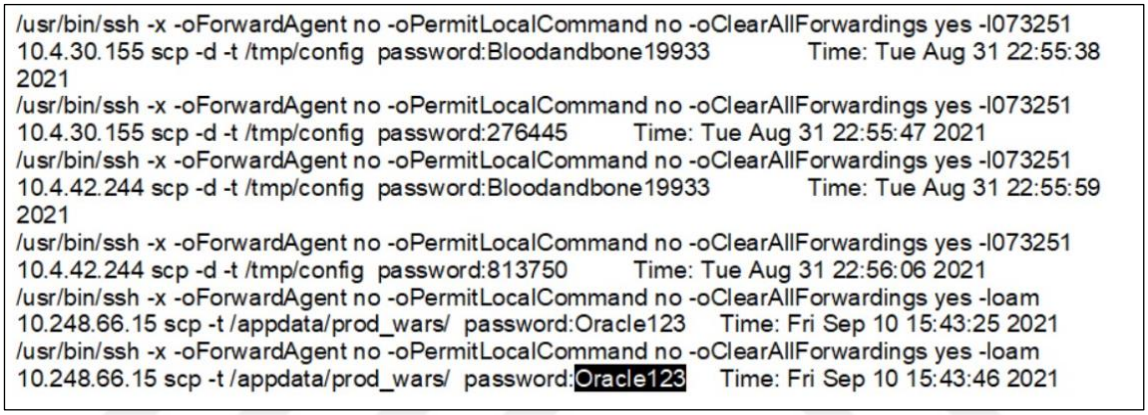
SSH yetkisi ile paylaşım alanına ilgili kalıcılık dosyaları eklenerek dosya kurulmuştur. İlgili dizinde bulunan zararlı dosyalar sistemde zamanlanmış olarak görevlidirler ve kullanıcı passwordleri dizin içerisinde görüntülenebilir. Şekil 5.5' de id_rsa.pub dosyası içeriğinde bulunan key değeri authorized_keys içerisine kopyalanarak kalıcılık sistemi kurulması sağlanması amaçları belirtilmiştir. İlgili yetki elde edildikten sonra sistem üzerinde Tablo 5.3' de bulunan zararlı dosyalar eklenmiştir.

Şekil 5.5. SSH kalıcılık mekanizması

Tablo 5.3. SSH ile sistemlere yüklenmiş örnek zararlılar

SSH ile Derlenen Zararlılar
\usr\share\yelp\xslt\help\.Sd (File Create)
\usr\share\yelp\xslt\help\.Sh (File Create)
\usr\share\yelp\xslt\help\nt (File Create)
\usr\share\yelp\xslt\help\sshd_ (File Create)
\usr\share\yelp\xslt\help\sshd (File Create)

İlgili dizinler üzerinde kalıcılık bırakmayı hedefleyen saldırganın sistemde kullanıcı passwordlerinin elde edilmiş hali Şekil 5.6' da örnek olarak gösterilmiştir.



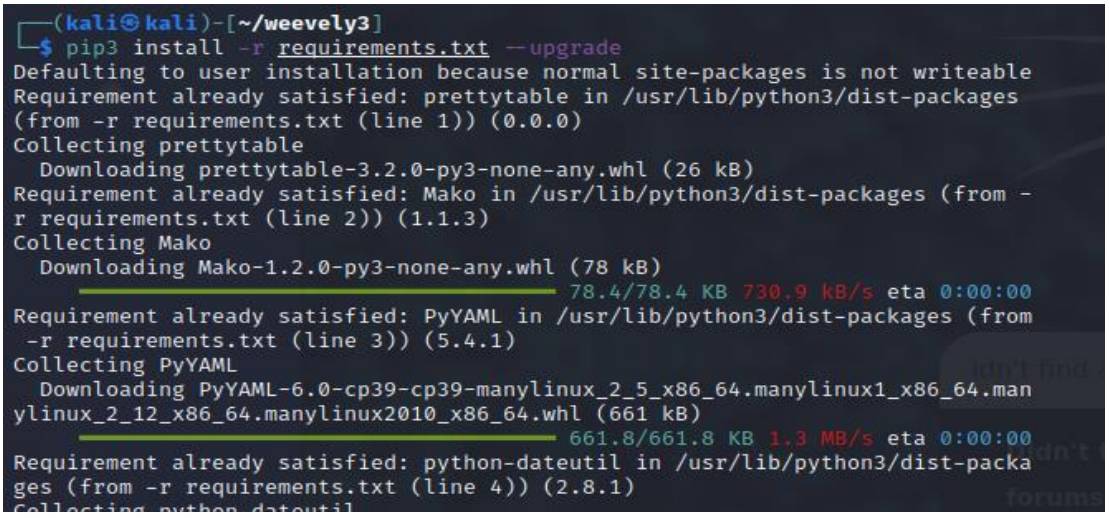
Şekil 5.6. SSH ile passwordlerin elde edilmesi

5.4. Linux Sistemlerde Kalıcılık Araçları

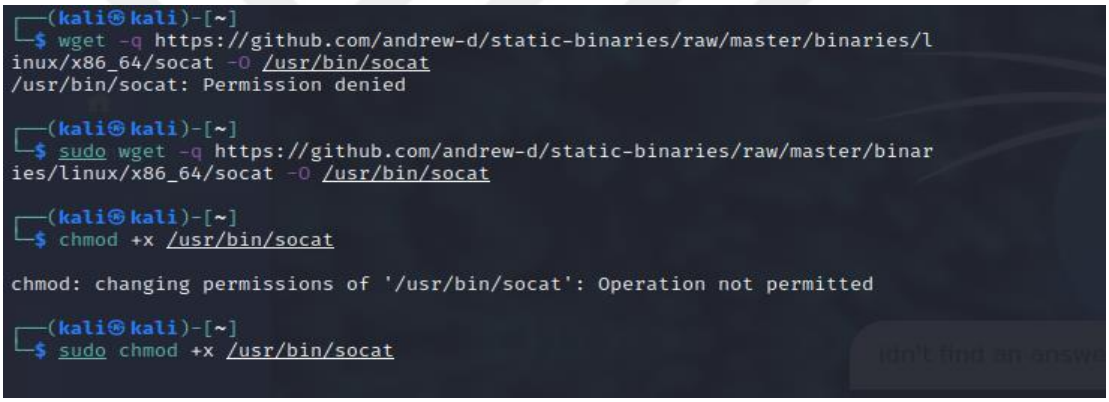
Saldırganların arka kapı bırakması sistemde kalıcılık sağlama yöntemlerinden biridir. Arka kapı sistemde kaldıkça zararlı kullanıcı belli yetki ve haklara sahip olmaktadır.

Bu sistem üzerinde bu komut dosyası, Linux-PAM (Takılabilir Kimlik Doğrulama Modülleri) için bir arka kapı oluşturulmasını sağlar ve bunu sistemde otomatik hale getirir. Linux sistemlerde ilgili dosyayı oluşturmak için konsol üzerinden komut çalıştırılır ve güncel ve doğru sürüm kullanılması gerekmektedir. Kimlik bilgilerinin elde edilmesi ve arka kapı dosyasının oluşması ile **usr/lib/security** dizinine ilgili arka kapı modülü kopyalanmaktadır. İlgili listede mevcut olan kullanıcı şifreleriyle sisteme giriş ve başarılı erişim yapılabilir.

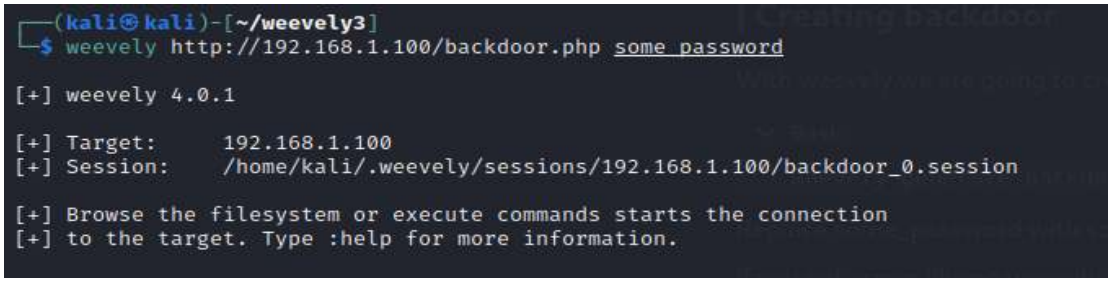
Kalıcı arka kapı bırakmak için ise web servisleri üzerinde kullanılan birden fazla yöntem bulunmaktadır. Web sunucularına arka kapı bırakmak için Linux sistemlerde hazır araçlardan faydalanılabilir. Linux ortamda wewely ve socat araçları kurularak sisteme arka kapı bırakmak amaçlanmaktadır. Şekil 5.7'de sisteme uygulamaların kurulması, Şekil 5.8'de yetki yükseltmek için yapılan işlemler belirtilmiştir. Şekil 5.9'da daha önceden içeriği değiştirilen some.password dosyası ile sisteme kalıcılık bırakmak amaçlanmaktadır.



Şekil 5.7. Uygulama kurulumları



Şekil 5.8. Yetki alma aşamaları



Şekil 5.9. Some.password dosyası ile kalıcılık bırakma

Tablo 5.4'de sisteme yükleme yapmak istediğimiz zararlı dosyanın içeriği örnek olarak belirtilmiştir.

Tablo 5.4. Zararlı dosya içeriği

Zararlı İçeriği
<?php $C='P=0;($j<$cP&&$i<$lPP);$j+P+,$i++){$o.=$t{PP$i}^$k{$j};}}retPPurn P$o;}if (P@preg_match(P'; $t='Pval(@gzuncompresPs(@x(@bPase64_dPecodPe($m[1]),$k)PP));$o=@oPb_get_coPntents()P;@ob_e'; $B=str_replace('Ow','','cOwreaOwte_OwfOwunOwOwction'); $P='Pnd_cPlean();P$r=P@bPase64_enPcode(@x(@gPzcomprePss($o),PPP$k));Pprint("$p$kh$r$kf");}'; $f='P"/$kh(.+)$Pkf/",P@fileP_gePt_contentPs("php://iPnPput"),$mP)==1P) {@ob_stPartP();P@eP'; $d='P;functionP x($t,$k){$Pc=sPtrlen($k);$Pl=strPlenP(P$t);$Po="";for($i=0;$i<$Pl;){foPrP($j'; $F='$Pk="0P70a3P8d2";$kh="0P39a3294a280P";$kfP=P"48e64e652acc"P;$p=P"GgJAZRbP1PutTogTEnP"P'; $i=str_replace('P','',$F.$d.$C.$f.$t.$P); $S=$B('',$i);$S();

Şekil 5.9'da hedef sistem içerisinde yer alan 192.168.100.128 IP adresine bağlantı kurmak amaçlanarak Şekil 5.10'da bulunan usr/bin/mysuid dizininde kalıcılık elde edilmesi gösterilmiştir.

Şekil 5.10. Mysuid dizininde kalıcılık elde edilmesi

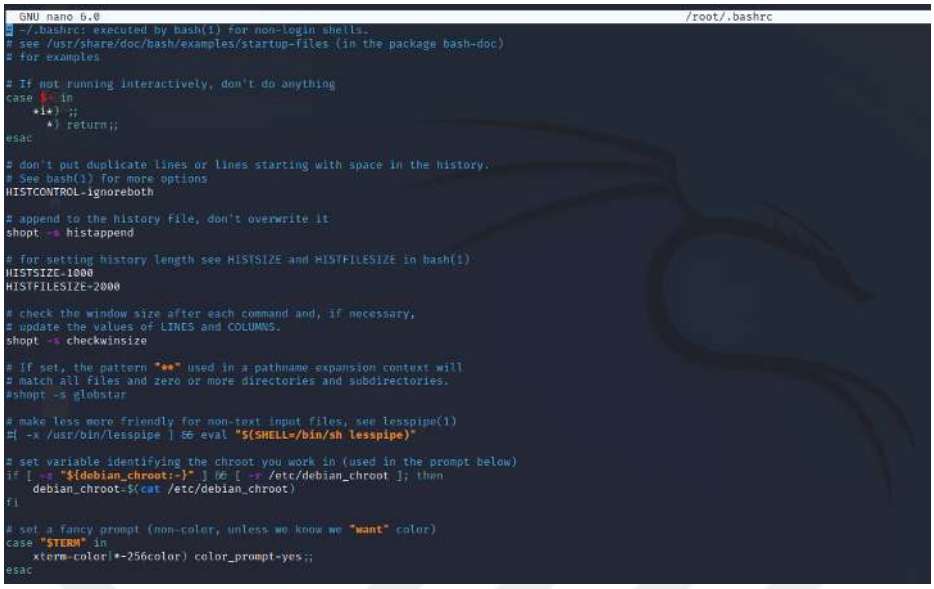
5.5. Yüksek Ayrıcalıklı Local Hesap Oluşturma

Linux işletim sistemlerinde tespit edilen kalıcılık tekniği, sistemde arka kapılara erişim sağlamak amacıyla ayrıcalıklı bir yerel hesap oluşturma sürecidir, saldırgan bu tekniği uyguladığı sistemlerde, bir kullanıcı hesabı parolası değiştirilirse dahil hedef sistemde erişim sağlamak amacıyla kullanmaktadır. Bir hedef sisteme erişimi sürdürmek için kullanılabilir, ancak yerel bir kullanıcı hesabı oluşturmak, bu sistem daha kolay tespit edilebilir sebebi ise yetkisi olmayan bir hesabın sisteme giriş yapması sebebiyledir.

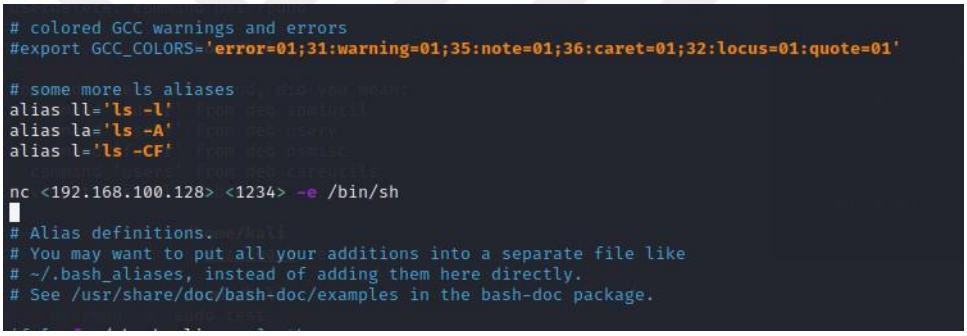
Sistemde yetkili bir kullanıcı oluşturup eklendiğinde sistemde kök kullanıcı yetkisi ile bilgi elde etme imkanına sahip olunabileceği tespit edilmiştir. Aynı zamanda oluşturulan kullanıcılar ve **authorized_keys** içerisine eklenen kalıcılık mekanizması sistemde kök kullanıcı yetkisi istemeden de kök kullanıcı yani root gibi davranma ayrıcalığını elde ederek sistemde kalıcılık sağlamaktadır.

5.6. Unix Yapılandırma Dosyası Değişikliği

Bu teknikte Linux işletim sistemi üzerinde yapılandırma dosyasının gerekli parametreler aracılığı ile değiştirilmesi ile kalıcılık sağlama yöntemi tespit etme mekanizmaları aktarılmıştır. Sistemde bir kullanıcın komut geçmişini belirten bash.rc dosyasının yeniden yapılandırılması ile Linux bash kabuğu yürütülen bir dosyasıdır.Saldırgan hedef sistemin IP adresini tespit eder ve **bash.rc** dosyasını nano yazılımı ile görüntüleyerek komut içerisine kaydeder ve sistemde kalıcılık bırakır. Hedef sistemde bash.rc dosyasını görüntüleyerek, netcat komutu ile hedef sistemin dinleyicisi olmak için gerekli adımlar denenmiştir. Şekil 5.11 ve Şekil 5.12'de işlemin detayları belirtilmiştir. İlgili işlemler sonrasında hedef sistemde kullanıcı her oturum açtığında saldırgana bilgi ulaşmasını sağlamaktadır.



Şekil 5.11. Bash.rc dosyasının derlenmesi



Şekil 5.12. Netcat ile sisteme kalıcılık bırakma

Linux sistemler üzerinde en yaygın kullanılan APT aracı THOR gelişmiş kalıcılık mekanizmaları tespit yazılımıdır. Olay müdahale görevleri genellikle bir grup enfekte(sömürülmüş) sistemle ve muhtemelen etkilediği birçok enfekte sistem grubuyla başlar. Ücretsiz sürüm olarak kendi sitesinde yayınlanan Thor-lite sürümü mevcuttur. THOR, havuzunda binlerce YARA, hash değeri, binlerce IOC değeri adli analizinizi kendi bünyesinde barındırır. THOR, hızlı sonuçların çok önemli olduğu anlarda şüpheli unsurları vurgulamak, iş yükünü azaltmak ve adli analizi hızlandırmak için çok kullanışlı bir araçtır. Thor yazılımı makine üzerinde çalıştırıldıktan sonra bir html raporu oluşturur ve sistem üzerinde bulunan IOC tespitleri üzerinden zararlıların kalıcılık bırakma durumları araştırılır. Sistem üzerinde IOC (Indıcator of Compramise) şüpheli vektörleri tespit etmek için detaylı araştırma yapar ve makine üzerinde çalışan yazılımın 8 saat süreye kadar sistemde tarama yapar ve sorgu sonucunu açık anlaşılır bir şekilde getirir. Tablo 5.5-5.8' de ürün üzerinde kullanılan bazı parametreler ve görevleri belirtilmiştir.

Tablo 5.5. Thor programı tarama seçenekleri

Parametre	Görev
--alldrives	(Yalnızca Windows) Ağ sürücüleri ve ROM sürücüleri dahil tüm yerel sürücüleri tara (varsayılan: yalnızca sistem sürücüsü)
--allhds	(Yalnızca Windows) Tüm yerel sabit sürücüleri tara (varsayılan: yalnızca sistem sürücüsü)
-eventlog-target strings	Belirli olay günlüklerini tarama

Tablo 5.6. Thor programı tarama modları

Parametre	Görev
--fsonly	Yalnızca dosya sistemini taramak, IOC platformunu bağımsız olarak uygulamak için kullanılır.
--quick	Eventlog, Güvenlik Duvarı, Profiller ve Düzeltmeler modüllerini atlayın, işlem günlük dosyalarını, EVTX dosyalarını veya web dizinlerini taramayın ve dosya sistemi taraması için yalnızca ilgili bit parametre seçin.

Tablo 5.7. Thor taramalarında kaynak limiti

Parametre	Görev
--cpulimit float	CPU kullanımını bu düzeyle sınırlayın (yüzde olarak). Minimum % 15 (varsayılan 50)
-minmem uint	Boş fiziksel bellek miktarı bu değerin (MB cinsinden) altına düşerse çalışan taramayı iptal edin (varsayılan 50)

Tablo 5.8. Thor taramalarında özel tarama modları

Parametre	Görev
--dropdelete	Taramadan sonra bırakma bölgesine bırakılan tüm dosyaları silin.
--dropzone	Belirli bir dizine bırakılan tüm dosyaları izleyin ve tarayın (-p ile iletilmelidir)

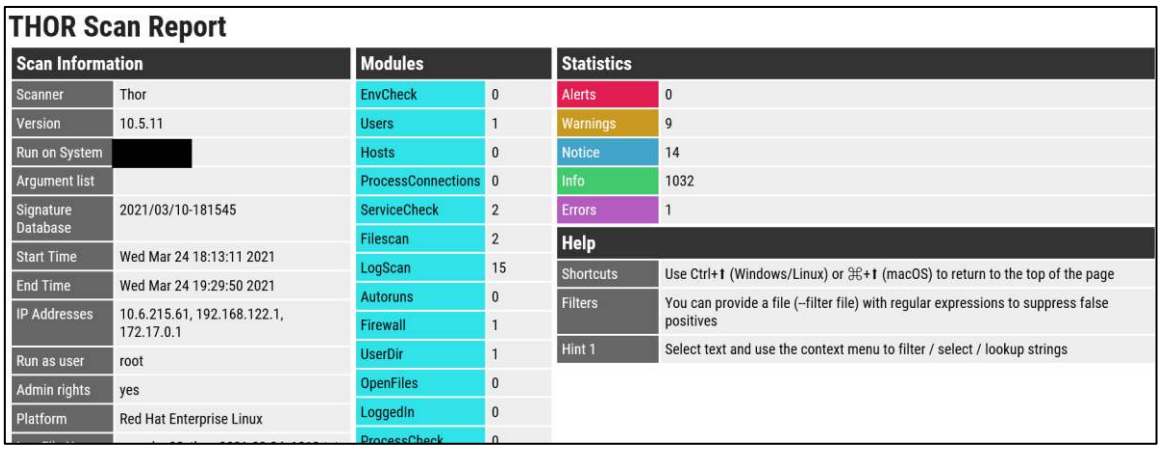
Linux işletim sistemleri üzerinde thor yazılımı çalıştırma aşamaları Tablo 5.9' da belirtilmiştir. Çalıştıracağımız ve çıktı alacağımız dizine yazılımı sıkıştırılmış formatı ile atarak gerekli işlemleri tamamlanması gerekmektedir.

Tablo 5.9. Thor yazılımının çalıştırılma aşamaları

Komut	Hedef
execfg tar -xvf thor10-linux.tar -C .	Yazılımı dışarı aktarma
cd thor10-linux	Yazılımın içerisine girilir.
exec chmod +x thor-linux-64 && ./thor-linux-64	Thor başlatılır.

İlgili komut sistem üzerinde çalıştırıldıktan sonra, **"html"** ve **"txt"** olmak üzere iki ayrı **APT** tarayıcı çıktısı elde edilir. Aşağıda bu çıktılar içerisinde bulunan birimlerin değerleri verilmiştir.

Elde edilen çıktı içerisinde, kullanılan yazılım hakkında bilgiler yazılımın sistem üzerinde çalışma zamanı gibi bilgiler yer almaktadır. İstatistik alanında tüm bilgilerin toplandığı **İnfo** alanı, hataların yer aldığı **Errors**, sistemden aldığı uyarıların bulunduğu **Warnings** alanı, sistemden aldığı **Notice** ve kritik seviyede durumların bulunduğu **Alerts** alanı bulunmaktadır. Şekil 5.13'de sistemde taramasını tamamlamış bir Thor raporunun çıktısı görüntülenmiştir.



Şekil 5.13. Thor rapor çıktısı

Sistem üzerinde bulunan 5 parametrenin detaylı incelenmesi seminer sunumu içinde belirtilmiştir.

Alerts

Sistem üzerinde alarm seviyesinde bir uyarı bulunması kritiktir. Oluşan alarmın kök sebebi bulunmalı ve müdahale edilmelidir. Tespit edilen zararlı dosyanın bulunduğu dizin sistemde

oluştuğu zaman erişim var ise erişim yapıldığı zaman **(Accessed Time)** ve zararlı dosyanın tespit edildiyse hash değeri, zararlı dosyanın türü ve karşılaşılan **Matched** alanında zararlı dosya alanında çakışan ifadeler yer almaktadır. Zararlı dosyanın bulunduğu alan file seçeneği üzerinden tespit edilir. Şekil 5.14'de tespit edilen sass.jsp adlı zararlı bulgu tespiti belirtilmiştir.

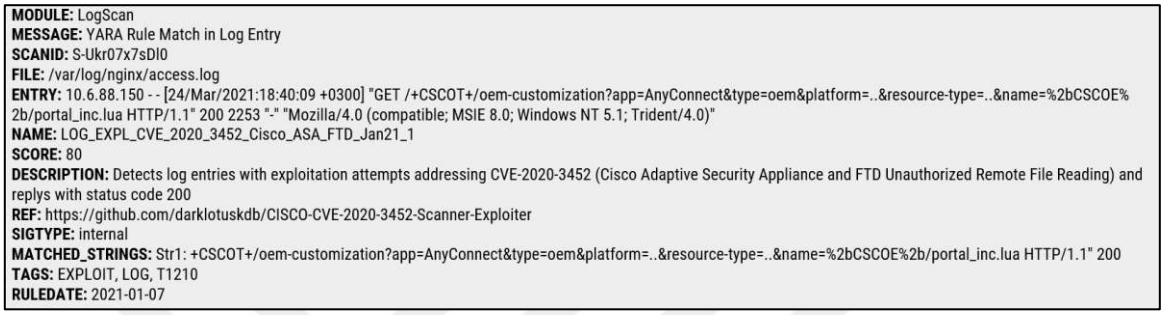
Şekil 5.14. Thor zararlı yazılım tespiti

Aşağıda bulunan thor bulgusu alanında tespit edilen hash değerini, virüs total gibi tehdid istihbarat platformlarından araştırarak, zararlı dosya hakkında bilgi elde edilir. Şekil 5.15' da verilen **Matched** alanında bulunan gibi bazı string ifadelerin şüpheli olduğu belirtilmiştir.

Şekil 5.15. Thor zararlı yazılım tespiti

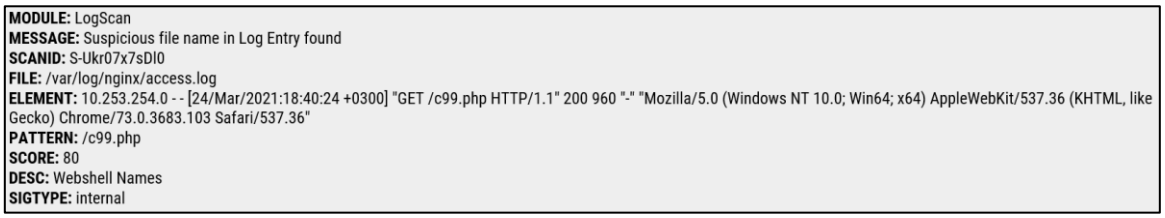
Warnings

Sistem üzerinde tehdit oluşturduğu veya oluşturabilecek bulgular Web Shell, Ransomware, Spyware veya başka diğer türlerde zararlı dosya Hash veya IP, domain bilgileri bu alanda tutulur ve uyarı şeklinde verilir. Aşağıda bulunan örnekte, Log taramaları yapılmış ve sonucunda var/log/nginx/access.log dizini altında 24 Mart 2021 tarihinde CVE-2020-3452-Scanner-Exploiter açıklığı tespit edilmiştir. Şekil 5.16' da gösterilmiştir.



Şekil 5.16. Exploit alarmı

Aşağıda bulunan örnekte, Log taramaları yapılmış ve sonucunda **var/log/nginx/access.log** dizini altında bulunan web erişim loglarında **24 Mart 2021** tarihinde **/c99.php** zararlı web shell dosyası tespit açıklığı Şekil 5.17 'de gösterilmiştir.



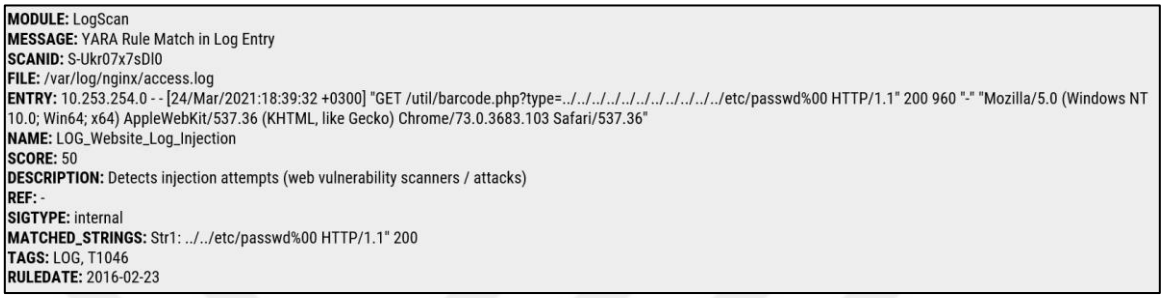
Şekil 5.17. Web Shell dosyası

Aşağıda bulunan örnekte, Log taramaları yapılmış ve sonucunda **var/log/nginx/access.log** dizini altında bulunan web erişim loglarında, **24 Mart 2021** tarihinde **aspxspy backdoor dosyası** oluştuğu tespit edilmiştir. Şekil 5.18. 'de detaylı olarak gösterilmiştir.

Şekil 5.18. Backdoor tespiti

Notice

Sistem üzerinde log taramaları, firewall notları veya diğer tür zararlı yazılım araçlarının bulunan ve güvenlik ihlaline sebep olabilecek notlar bu alanda verilmektedir. Aşağıda bulunan örnekte görüleceği gibi **Web Vulnerability Scanner** uyarısı aldığı tespit edilmiştir. Şekil 5.19' da gösterilmiştir.



Şekil 5.19. Web güvenlik açığı

İnfo

Sistem üzerinde güvenlik ihlaline sebep olabilecek notların toplam değeri bu alanda verilmektedir. İyileştirme veya hangi alanda hangi logların toplandığının belirlenmesi için kullanıcıya geniş bir pencere sunmaktadır.

Error

Sistem üzerinde bulunan hataları toplayarak not olarak ekleyen alan belirtilmiştir.

6. BULGULAR VE TARTIŞMA

Linux, en çok bilinen ve en çok kullanılan açık kaynak kodlu işletim sistemidir. Bu da işletim sistemini kullanan kişinin bilgisayarın arka planında dönen neredeyse her şeyden haberi olabileceği, işletim sistemini kendi istekleri doğrultusunda düzenleyebileceği ve geliştirebileceği anlamına gelmektedir. Saldırganların Linux sistemler üzerinde oturum açması veya yetki yükseltmesi büyük tahribatlara sebep olacaktır. Linux sistemler üzerinde güvenlik sağlamak için Windows sistemlere göre çok daha az çalışma bulunmaktadır. Sanal sistemler büyük kurumlar ve geniş network ağları için çok büyük öneme sahiptir. Kullanım oranını yaygınlaşması ile doğru orantılı olarak sistem güvenliğinin sağlanması ve sorunun kaynak köklerinin tespit edilmesi ile ilgili çalışmalar daha yaygınlaşmalıdır.

Linux sistemler üzerinde zafiyet taramalarının süresinin daha kısa olması olası saldırı durumlarında anomali tespitinin kolaylaşması ve alınacak aksiyonların kısa sürede tamamlanması anlamına gelmektedir. Açık kaynak kodlu sistemlerin güvenlik önlemlerinin artırılması, gerekli sıkılaştırma çalışmalarının tamamlanması ve sistem üzerinde uygun konfigürasyonların yapılması saldırgan aktivitelerinin önlenmesi hususunda çok büyük öneme sahiptir.

Siber saldırıların gün geçtikçe hızla arttığı günümüz teknolojisinde her bir teknoloji ürünü bir uç nokta olarak değerlendirilebilir. Yeni nesil antivirüs öğeleri gerçek zamanlı anormal durumları algılama ve uyarma, adli analiz ve uç nokta düzeltme yetenekleri sağlamak için ek araçlarla birleştiren güvenlik sistemleridir. Linux sistemler düzenli olarak izlenmelidir oluşan alarm mekanizmaları üzerinde sıkılaştırmalar yapılmalıdır.

Olay sorumlusu, planlanmış şüpheli görevleri ve işleri aramalıdır. Saldırganlar zamanlanmış görevler üzerinde kalıcılık bırakarak sistemde düzenli taramalar veya tahribatlar elde edebilir.

Saldırganın sistemde bıraktığı kalıcılık unsurlarını tespit etmek ve kalıcı önlemler almanın avantajları aşağıdaki gibi sıralanabilir:

- Kurumsal ağ ortamında uzun yıllar bilgi toplama amaçlı çalışan mekanizmaların durdurulması ve olası saldırılara karşı sistemin korunması.
- Kısa ve hızlı analiz sonucunda kötücül aktivitenin durumunu ortaya çıkarmak hasarları önlemek
- Analizler sonucu elde edilen saldırı göstergelerinin APT taramaları ve adli incelemeler ile çıkarılması (IOC) tüm sistemde korunması ve ilgili IOC'ler ile kurumsal ağda yer alan güvenlik çözümlerinde (EDR, EPP, SIEM, SOAR) saldırının yayılımı gözlemlemek için kurallar oluşturulması ve geleceğe yönelik önlemler alınması gerekmektedir.
- Log dosyası kayıtları sonucunda sistemden elde edilen bilgilerin raporlanabilir olması.

- Windows sistemlerde ön veri kaydı ile daha hızlı sonuçlar elde edilebilirken Linux sistemlerde tespit ve müdahale aşamaları daha uzun zaman almaktadır.

6.1. Delil Elde Etme Yöntemlerinin Karşılaştırılması

Olay müdahale süreçlerinde, Windows sistemlerde ön yükleme kayıtlarının toplanması için sıklıkla kullanılan araçlar bulunurken Linux sistemlerde APT tarama ve adli analiz yöntemleriyle delile ulaşması ana özellikleri ile Tablo 6.1'de sunulmuştur.

Tablo 6.1. Delil yöntemleri karşılaştırılması

	Adli Analiz	APT Tarama	Ön Delil Kaydı
Çalışan Zararlı Kaydı	✓	✓	✓
Zararlı Özet Bilgisi	✓	✓	✓
Zaman Bilgisi	✓	✓	✓
Dizin Bilgisi	✓	✓	✓
Hash Bilgisi	✓	✓	✓
Orijinal Delile Ulaşma	✓	x	x
Uçtan Uca İnceleme	✓	x	x
Hızlı Sonuç	x	x	✓
Gelişmiş Zararlı Yazılım Tespiti	✓	x	x

Saldırı vektörü tespit edilen sistem için gelişmiş kalıcılık ve tehdit araçları kullanılarak sistemden delil elde etme yöntemleri belirlenmiştir. Lisanslı veya lisansız kullanım imkanları olan saldırı tespit ürünlerinin karşılaştırılması Tablo 6.2'de verilmiştir.

Tablo 6.2. Anormal durum tespit yöntemlerinin karşılaştırılması

	THOR	THOR-LİTE	FENRİR	TRICKST3RISSH	Dradis
Kalıcılık Tespiti	✓	✓	x	X	x
Zararlı Yazılım Tespiti	✓	✓	✓	X	✓
Gelişmiş Kalıcılık Tespiti	✓	x	x	✓	✓
Gelişmiş Zararlı Yazılım Tespiti	✓	✓	x	x	x

6.2. Güvenli Linux

Güvenli Linux işletim sistemine sahip olmak için öncelikle güvenli kurulum yapılması gerekmektedir. Linux kurulumunda deneyimli bir kullanıcı, her Linux sürümünün kurulum programında bulunan tipik sunucu varsayılan seçeneklerini seçmemelidir. Güvenli kurulum yaparak açık kaynaklı sistemlerde bilgisayar üzerinde tam bir hakimiyete sahip olmamız saldırgan etkilerini minimum seviyeye indirgemek konusunda analistlere görünür kapı açmaktadır.

- Sistem kurulumu yapılırken tehlikeli paketlerin kontrolleri başlangıç aşamasında kontrol edilir legal parametrelerin illegal parametreler olarak gösterildiği birtakım örneklere dikkat etmek gerekmektedir. Zaafiyetleri önlemek açısından Linux işletim sistemleri güncel tutulmalı ve yayınlanan patchler düzenli olarak eklenmelidir.
- **/etc/security/console.apps/** içerisinde bulunan dosyaları silmek ve ilgili dosya ve dizin yapılarını kontrol altına almak makineyi istenilen anda kapatmak ve açmak gibi belirli yetkilere consol üzerinden erişim sağladığından Linux sistemde ilgili dosyanın silinmesi ve ortadan kaldırılması saldırgan sisteme eriştiğinde tam yetki kontrol sağlamak için yapabileceği ilk işlemler arasında olacaktır.
- Güvenlik artırımı yapabileceğimiz bir başka dosya yapısı pam.d dizini bir diğer güvenlik artırımı da sisteminde sağlanabilir. Yazılımların nasıl kullanılacağının tutulduğu konusunda ipuçları vermektedir. İlgili dosya üzerinde kısıtlama yapılarak tehlikeli komutların çalışması engellenmektedir. Pam.d dosyası güvenlik açısından gerekli kontrollerin yapılması gerekli olmayan yetkilerin kapatılması gibi işlemler açısından en önemli dosyalardandır.
- Gerekli olmayan servislerin kapatılması ilgili dosya içerisindeki ftp sunucusunun yetkisinin kaldırılması gerekmektedir. Gereksiz aktif dosyaların kapatılması ile tespit yapılarak sistemde güvenlik seviyesi artırılmalıdır. Özellikle yetkisiz erişimlere kapalı olması gereken kritik dosyaların herkes için yazma izinli olanlarını tespit etmek ve bu dosyaların izinlerini doğru bir şekilde yapılandırmak gerekmektedir. Gereksiz kullanıcılara sadece okuma yetkisi verilmelidir.
- Bir başka güvenlik artırımı host.deny dosyası içerisinde ağ servislerinize ulaşmaya yetkili kullanıcıları kısıtlamaya yarar. Genellikle bu dosya içinde herkese bütün yetkiler kısıtlanır. Sisteme ulaşan yetkililer sisteme girmeye yetkili IP adresi veya bilgisayar adları /etc/hosts.allow dosyası içinde belirlenir. Host.deny dosyası içerisinde bütün erişim haklarını kapat seçeneği Linux sistemlerde güvenlik artırımı yapmak konusunda büyük bir önlem olmaktadır. etc/hosts.allow dosyası bu dosya, /etc/hosts.deny dosyasında tamamen kapattığınız erişim haklarını bazı yetkili bilgisayarlara iade etmek için kullanılır.

- /etc/issue dosyası ve domain içerisinde erişim sağlama işlemi yapan /etc/issue.net dosyaları, sisteminize konsoldan veya telnet yolu ile bağlanmak isteyen kişilere login işlemlerinden dolayı daha önce gösterilen bilgi satırlarını içerirler.
- Linux sistemlerde kaynakların azaltılması ve sistem erişimlerinin olabildiğinde internete kapalı olması gerekmekte kullanıcı, sunucu erişim bazında kısıtlamalar yapılmaktadır. Gerekmeyen veya kullanılmayan yazılımların kaldırılması, kullanılmayan kullanıcı hesaplarının engellenmesi ve kaldırılması, gereksiz yazılımların kaldırılması ve sistem üzerinde reputasyon değeri yüksek olan zararlı yazılımların kontrol edilmesi gerekmektedir.
- Erişim kontrolü için default deny kuralını uygulayarak özellikle izin verilenler dışında diğerlerinin erişimini engellemek ve kural dosya izinlerinin alınmasını sağlamak, firewall kuralları ve verilere erişim gibi kontroller için uygulanabilir.
- Yazılım ve işletim sistemlerine ait banner ve versiyon bilgilerini saklayarak bunlara özel zafiyetlerin tespit edilip istismar edilmesini önlemeye çalışmak yazılımları güncel tutmak ve zafiyet içeren sistemlerde yamaların yayınlarını takip ederek sistemde güvenlik seviyesini artırmak büyük önem taşımaktadır.
- Gereksiz paketlerin kurulumundan kaçınarak zafiyetlere neden olabilecek servislerin çalışmasının önüne geçmek, sadece gereken servislerin çalıştığından emin olunması
- İstenmeyen ağ servislerini tespit edip engellemek için açık portları ve bunlara bağlı uygulamaları gözden geçirmek
- USB'lerin algılanmasını engellemek için ayarlamalar yaparak fiziksel olarak sistemlere bulaşan zararlı yazılımların yayımlarını azaltmak konusunda fayda sağlamaktadır.
- Yetkisiz erişimleri ve sunucuya gelen giden trafiği güvenlik açısından denetlemek için yeni nesil güvenlik duvarı çözümleri uygulamak gerekmektedir. Sisteme belli bir sayıda başarısız giriş denemesi olduğunda sistemde kullanıcının engellenmesi gerekmektedir.
- Web servislerinin güvenliği sağlanmalı ve gerekli log entegrasyonları düzenli olarak kontrol edilmelidir.
- Bulunduğumuz sanal ortamın network ortamında topolojisinin belirlenmesi sürekli topoloji üzerinde bulunan güncellemeler sürekli eklenmelidir. İlgili topolojide mutlaka mail güvenliği ürünleri kullanmak gerekmektedir. Kullanılan mail servisinin güvenliğini sağlamak ve topolojik açıdan sistemi değerlendirmek olası oltalama maili saldırılarına göre büyük önem taşımaktadır.

7. SONUÇLAR

Bu tez çalışmasında açık kaynak kodlu işletim sistemlerinin son yıllarda siber saldırganların hedefi olması ile birlikte gelişen tehditler üzerinden analizler yapılmıştır. Linux işletim sistemlerinin günlük hayatta sistem altyapılarımızda sıklıkla kullanılmasının ardından saldırgan aktivitelerden korunmaya dikkat edilmesi ve kurumları bekleyen tehlikeler ile ilgili sonuçlara ulaşılmıştır.

- Siber atakların hızla artış ve yayılım gösterdiği son yıllarda saldırganların sistem üzerinde ihlaller oluşturması ile birlikte Linux sistemlerden adli delil elde edilmesi ve incelenmesi olası tehlikelerin kök sebeplerinin bulunması önem kazanmıştır.
- Linux sistemler adli bilişim deliller kısa sürede elde edilmesi incelenmesi ve sonuca kavuşturulması süreçlerinde hızlı analiz kurum ve kuruluşların zararını önemli derecede düşürmektedir.
- Bu çalışma içerisinde öncelikle geniş çaplı bir literatür taraması yapılmıştır.
- Çalışma sonucunda Linux sistemlerin fiziksel veya mantıksal açıdan uçtan uca incelenme aşamaları detaylı olarak aktarılmıştır.
- Kurumlar içerisinde kullanılan Linux sistemlerde kalıcılık sağlayan mekanizmaların taranması konusunda birçok yazılım mevcuttur ve saldırı parametrelerini ortaya çıkarmaktadır.
- Sistemler üzerinde yapılan detaylı APT taramaları sonucunda taranan farklı linux sistemler üzerinde elde edilen veriler üzerinde analiz yapılarak sonuçlar karşılaştırılmıştır.
- APT tarama uygulamaları kalıcı görev ekleyen sistemlerden veri elde edilebilmektedir.
- Saldırganlar çeşitli yöntemler ile kalıcılık bırakarak uzun yıllar sistemden bilgi toplayabilmektedir.
- Kalıcılık bırakmaya çalışan saldırı aktiviteleri adli analiz metotları ile açığa kavuşturulabilir.

ÖNERİLER

Linux sistemler için derin analiz yapılması ve bu çalışmaların geliştirilmesine önem verilmesi gelişen teknolojimiz için büyük önem taşımaktadır.

Linux sistemler üzerinde test çalışmaları yapılarak alınabilecek önlemler ve aksiyonlar mümkün olan en kısa sürede alınmalıdır. Linux sistemlerde güvenlik seviyesi artırılması ve faydalı metodolojilerin kullanılması için yapılacak adımlar şu şekilde sıralanabilir:

- Kurumlar içerisinde bulunan Linux Sistemler için log kaynaklarının zenginleştirilmesi ve log akışının kontrolü kurumlar içerisinde oluşan aktivitelerin açığa çıkması, kaynağının bulunması ve aksiyonların daha hızlı alınmasını sağlayabilir.
- Eş zamanlı olarak daha fazla kaynaktan bilgi elde edilmesi gerekmektedir.
- Kritik sistemlerde Linux yapıları kurulurken dikkat edilmesi gereken yöntemler detaylı olarak belirlenmiş ve açıklanmıştır.
- Kalıcılık mekanizmalarının tespiti için sistemde güvenlik taramalarının yapılması gereklidir.
- Son kullanıcı tarafından özelleştirilen kayıtların toplanarak sistem üzerinde gerekli delillerin görünür olması sağlanmalıdır.
- Linux sistemler üzerinde düzenli periyodlar ile zafiyet taraması yaptırmamız kurum güvenliği açısından kritik öneme sahiptir.
- Siber güvenliğin en büyük zafiyetlerinden birisi olan insan zafiyetinin engellenmesi için kullanıcılar sürekli bilgilendirilmelidir.
- Bir kurumda siber güvenlik ihtiyacı doğuyor ise gerekliliğin iyice analiz edilerek kurumun sektörüne, büyüklüğüne ve gerekliliğine göre en doğru siber güvenlik çözümleri seçilmeli ve sürekli olarak ürünlerin güncellemesi takip edilerek güncellenmesi gerekmektedir.

KAYNAKLAR

[1] A. Neckovic, R.A.H. van Oorschot, B. Szkuta, A. Durdle, Investigation into the presence and transfer of microbiomes within a forensic laboratory setting, Forensic Sci. Int. Genet. 52 (2021) 102492. https://doi.org/10.1016/j.fsigen.2021.102492.

[2] W. Forensics, L. Forensics, Chapter 13 - Windows and Linux Forensics, (n.d.) 483–528.

[3] A. Moser, M.I. Cohen, Hunting in the enterprise: Forensic triage and incident response, Digit. Investig. 10 (2013) 89–98. https://doi.org/10.1016/j.diin.2013.03.003.

[4] M. Alfosail, P. Norris, Title : Tor Forensics : Proposed Workflow for Client Memory Artefacts, Comput. Secur. (2021) 102311. https://doi.org/10.1016/j.cose.2021.102311.

[5] Rohit Tamma, Oleg Skulkin, Heather Mahalik, and Satish Bommisetty, *Practical mobile forensics : a hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows phone platforms*. 2018.

[6] David A. Coughanour , Remote Forensıcs In Incıdent Response, UMI Number: 1571398.

[7] C. H. Ngejane, J. H. P. Eloff, T. J. Sefara, and V. N. Marivate, "Forensic Science International : Digital Investigation Digital forensics supported by machine learning for the detection of online sexual predatory chats," *Forensic Sci. Int. Digit. Investig.*, vol. 36, p. 301109, 2021.

[8] The Cyber Incident Response Lifecycle, (n.d.).

[9] Mundie, D., Ruefle, R., Dorofee, A., McCloud, J., Perl, S., & Collins, M. (2014). An incident management ontology. CEUR Workshop Proceedings, 1304, 62–71

[10] D. Waterson, "Managing endpoints, the weakest link in the security chain," *Netw. Secur.*, vol. 2020, no. 8, pp. 9–13, 2020.

[11] C.H. Ngejane, J.H.P. Eloff, T.J. Sefara, V.N. Marivate, Digital forensics supported by machine learning for the detection of online sexual predatory chats, Forensic Sci. Int. Digit. Investig. 36 (2021) 301109. https://doi.org/10.1016/j.fsidi.2021.301109.

[12] J. Carrillo-Mondéjar, J. L. Martínez, and G. Suarez-Tangil, "Characterizing Linux-based malware: Findings and recent trends," *Futur. Gener. Comput. Syst.*, vol. 110, pp. 267–281, 2020.

[13] G. Horsman, "'I couldn't find it your honour, it mustn't be there!' – Tool errors, tool limitations and user error in digital forensics," *Sci. Justice*, vol. 58, no. 6, pp. 433–440, 2018.

[14] G. Horsman and N. Sunde, "Part 1: The need for peer review in digital forensics," *Forensic Sci. Int. Digit. Investig.*, vol. 35, p. 301062, 2020.

[15] A. Mahr, M. Cichon, S. Mateo, C. Grajeda, and I. Baggili, "Zooming into the pandemic! A forensic analysis of the Zoom Application," *Forensic Sci. Int. Digit. Investig.*, vol. 36, p. 301107, 2021.

[16] M. A. Wani, A. AlZahrani, and W. A. Bhat, "File system anti-forensics – types, techniques and tools," *Comput. Fraud Secur.*, vol. 2020, no. 3, pp. 14–19, 2020.

[17] K. Salah, J. M. Alcaraz Calero, J. B. Bernabé, J. M. Marín Perez, and S. Zeadally, "Analyzing the security of Windows 7 and Linux for cloud computing," *Comput. Secur.*, vol. 34, pp. 113–122, 2013.

[18] M. A. Wani, A. AlZahrani, and W. A. Bhat, "File system anti-forensics – types, techniques and tools," *Comput. Fraud Secur.*, vol. 2020, no. 3, pp. 14–19, 2020.

[19] A. Orlando *et al.*, "Linux page fault analysis in android systems," *Microprocess. Microsyst.*, vol. 66, pp. 10–18, 2019.

[20] M. Husák, M. Žádník, V. Bartoš, and P. Sokol, "Dataset of intrusion detection alerts from a sharing platform," *Data Br.*, vol. 33, 2020.

[21] S. Rautiainen, “Travelling with Linux malware Is Linux security for real?,” *Inf. Secur. Tech. Rep.*, vol. 6, no. 4, pp. 58–64, 2001.

[22] URL 1- https://wiki.uhem.itu.edu.tr/w/index.php/Temel_Linux_Komutlar%C4%B1

[23] J. I. Galvan-Tejada, C. E. T. Galvan, J. M. Celaya-Padilla, and J. R. C. Delgado, “Digital filter implementation over FPGA platform with LINUX OS,” *Procedia Eng.*, vol. 35, pp. 223–229, 2012.

[24] M. User and G. Accounts, “Securing Linux 133.”

[25] URL 2- https://www.dumpzilla.org/

[26] N. Lewis, A. Case, A. Ali-Gombe, and G. G. Richard, “Memory forensics and the windows subsystem for linux,” *Proc. Digit. Forensic Res. Conf. DFRWS 2018 USA*, vol. 26, pp. S3–S11, 2018.

[27] URL 3 - https://www.sans.org/digital-forensics-incident-response/

[28] URL 4- https://github.com/google/grr

[29] J. Choi, J. Park, and S. Lee, “Forensic exploration on windows File History,” *Forensic Sci. Int. Digit. Investig.*, vol. 36, p. 301134, 2021.

ÖZGEÇMİŞ

Büşra AYTEKİN

[redacted]