Kadirli Uygulamalı Bilimler Fakültesi Dergisi
Cilt 4, Sayı 1, 210-226, 2024

Journal of Kadirli Faculty of Applied Sciences
Volume 4, Issue 1, 210-226, 2024

Kadirli Uygulamalı Bilimler Fakültesi Dergisi

Journal of Kadirli Faculty of Applied Sciences

Siber Güvenlikte Kali Linux ve Sızma Araçlarının Kullanımı

Hakan ETİK[1], Özgü CAN[2*]

[1]Ege Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Fakültesi, İzmir
[2]Ege Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Fakültesi, 35100 Bornova-İzmir

[1]https://orcid.org/0009-0003-0589-9756
[2]https://orcid.org/0000-0002-8064-2905
*Sorumlu yazar: ozgu.can@ege.edu.tr

Araştırma Makalesi

Makale Tarihçesi:
Geliş tarihi: 21.07.2023
Kabul tarihi: 06.12.2023
Online Yayınlanma: 08.03.2024

Anahtar Kelimeler
Siber güvenlik
Güvenlik açığı
Kali Linux
Sızma araçları
Bilişim güvenliği

ÖZ

Siber güvenliğin sağlanmasında Kali Linux ve sunduğu sızma araçlarının sunucu sistemlerine yönelik penetrasyon testlerinde kullanımı önemlidir. Bu çalışmada, test ortamı olarak Linux Ubuntu işletim sistemi ve üzerinde çalışan bir web sunucusu kullanılmıştır. Test ortamında, Kali Linux üzerindeki sızma araçları kullanılarak yapılan tüm tarama ve sızma işlemleri gerçekleştirilmiştir. Öncelikle, hedef sistem üzerindeki açık portları tespit etmek için port taraması uygulanmıştır. Tarama ile sistemdeki aktif servisler ve servislerin çalıştığı portlar belirlenmiştir. Sonraki adımda, kullanıcı adı ve parola kombinasyonlarının bir listesi kullanılarak oturum açma bilgilerini elde etmek hedeflenmiştir. Sözlük saldırısı ile parola kırma işlemi yapılmıştır. Böylelikle, zayıf parolaların kullanıldığı hesapların belirlenmesi gerçekleştirilmiştir. Çalışma kapsamında ayrıca, SQL saldırısı gerçekleştirilerek hedef sistemin veritabanına yetkisiz erişim sağlanmıştır. Saldırı yöntemiyle güvenlik açıklarının olduğu web uygulamaları hedef alınarak veritabanına sızma girişiminde bulunulmuştur. Veritabanına erişim sağlandıktan sonra hassas verilere erişilmiş ve veriler manipüle edilmiştir. Son olarak, yetki yükseltme işlemi gerçekleştirilerek hedef sistemin tam kontrolünün ele geçirilmesi sağlanmıştır. Sistemdeki zayıf yapılandırmalar, güvenlik açıkları veya yetkilendirme hatalarının tespit edilmesi hedeflenmiştir. Sonuç olarak, Kali Linux ve sızma testi araçlarının sunucu sistemlerindeki güvenlik açıklarını tespit etmek ve gidermek için önemli bir araç olduğu gösterilmektedir. Çalışmanın sonuçları, Kali Linux ve sızma testi araçlarının güçlü yeteneklerini ve potansiyel güvenlik açıklarını ortaya çıkarmada etkinliğini göstermektedir. Böylelikle, sistem yöneticileri benzer araçları kullanarak yönettikleri sistemleri test ederek güvenlik açıklarını tespit edebilir ve gerekli önlemleri alabilirler. Bu çalışmada, bu önemin açıklanması ve oluşturulan deneysel test ortamında gösterilmesi hedeflenmektedir.

Using Kali Linux and Infiltration Tools in Cyber Security

Research Article

Article History:
Received: 21.07.2023
Accepted:06.12.2023
Available online: 08.03.2024

Keywords:
Cyber security

ABSTRACT

It is important to use Kali Linux and the penetration tools that it offers in penetration tests for server systems to ensure cyber security. For this purpose, Linux Ubuntu operating system and a web server running on it are used as test environment. In this test environment, all scans and penetrations are performed using the penetration tools on Kali Linux. First, port scanning is performed to detect open ports on the target system. With this scan, the active

Vulnerability
Kali Linux
Penetration tools
IT security

services in the system and the ports where these services are running are determined. The next step is to obtain login information using a list of username and password combinations. Password cracking with dictionary attack is performed. Thus, the identification of accounts with weak passwords is achieved. Unauthorized access to the database of the target system is achieved by performing a SQL attack. With this attack method, an attempt is made to infiltrate the database by targeting web applications with security vulnerabilities. After accessing the database, sensitive data is accessed and manipulated. Finally, full control of the target system is achieved by performing privilege escalation. In this step, weak configurations are aimed to detect vulnerabilities or authorization errors in the system. Consequently, Kali Linux and penetration testing tools are an important tool for detecting and resolving vulnerabilities in server systems. The results of the study show the powerful capabilities of Kali Linux and penetration testing tools and their effectiveness in determining potential vulnerabilities. Thus, system administrators can use such tools to detect vulnerabilities and take the appropriate actions by testing the systems they manage. In this study, it is aimed to explain this importance and to show this in an experimental test environment.

To Cite: Etik H, Can Ö., 2024. Siber güvenlikte kali linux ve sızma araçlarının kullanımı**.** Kadirli Uygulamalı Bilimler Fakültesi Dergisi, 4(1): 210-226.

Giriş

Günümüzde güvenlik açıklarının tespit edilmesi ve kapatılması büyük bir önem taşımaktadır. Kurumlar ve bireyler; bilgisayar sistemlerini, ağlarını ve uygulamalarını potansiyel tehditlere karşı korumak için güvenlik testlerine ihtiyaç duyarlar. Bu ihtiyaca cevap veren sızma testi (penetrasyon testi), güvenlik açıklarının belirlenmesi ve hedef sistemlere yetkisiz erişim sağlanarak gerçekleştirilen saldırı senaryolarını içerir.

Bu çalışmada kullanılan Kali Linux, özel olarak sızma testi ve etik saldırılar için tasarlanmış bir Linux dağıtımıdır. Kali Linux içerisinde birçok güvenlik aracı ve kaynak bulundurur ve sızma testi süreçlerinde kullanıcıya esneklik ve güç sağlar.

Sızma testleri, bir organizasyonun veya bireyin sistemlerini güvenli hale getirmek için proaktif bir yaklaşımı temsil eder. Bu testlerde, gerçek dünya saldırı senaryolarının gerçekleştirilmesi ve potansiyel zayıf noktaların belirlenmesi hedeflenir. Kali Linux, güvenlik testlerinde kullanılabilecek birçok araç sunar: Ağ taraması, zayıf parola analizi, güvenlik açığı taramaları, ağ saldırıları, veritabanı güvenliği, kablosuz ağ güvenliği ve daha fazlası gibi alanlarda uzmanlaşmış araçlara erişim sağlar.

Bu çalışmanı kapsamı sızma testi süreci, planlama, bilgi toplama, zafiyet taraması, saldırı senaryolarının oluşturulması gibi temel adımları içermektedir. Her adımın nasıl gerçekleştirileceği ve hangi araçların kullanılacağı ayrıntılı bir şekilde açıklanmaktadır. Sızma testleri, organizasyonların güvenlik politikalarını güncellemelerine ve potansiyel riskleri azaltmalarına yardımcı olmaktadır. Çalışmanın sonuçları da sızma testlerinin önemini ve etkinliğini vurgulamaktadır. Sızma testleri, hedeflenen sistemlerin güvenlik açıklarını tespit

etmek ve bunlara karşı önlemler almak için önemli bir araçtır. Sızma testleri, bilgi güvenliği konusunda sürekli bir çaba gerektiren ve tehditlere karşı savunma mekanizmalarını güçlendiren bir disiplindir.

Çalışmada Kali Linux kullanarak gerçekleştirilen bir sızma testi süreci detaylı bir şekilde sunulmaktadır. Çalışmada, Ubuntu 14.0 üzerinde çalışan bir web sunucusu hedef alınmış ve farklı sızma testi adımları kullanılarak saldırı senaryoları gerçekleştirilmiştir. Bu adımlar arasında port taraması, parola kırma, SQL saldırısı ve yetki yükseltme gibi işlemler yer almaktadır. SQL saldırısı, bir web uygulamasının arkasındaki veritabanına yönelik olarak gerçekleştirilen bir saldırı türüdür. Yetki yükseltme ise bir sisteme veya uygulamaya ait sınırlı bir erişim düzeyinin yetkisiz şekilde daha yüksek bir seviyeye yükseltilmesi işlemidir.

Sızma testi süreci Kali Linux ve sızma testi araçlarının kullanımı üzerinde odaklanmaktadır. Çalışmanın sonuçları sızma testlerinin önemini, güvenlik açıklıklarını tespit etmek ve gidermek için bu tür testlerin düzenli olarak yapılması gerektiğini vurgulamaktadır.

Materyal ve Metod

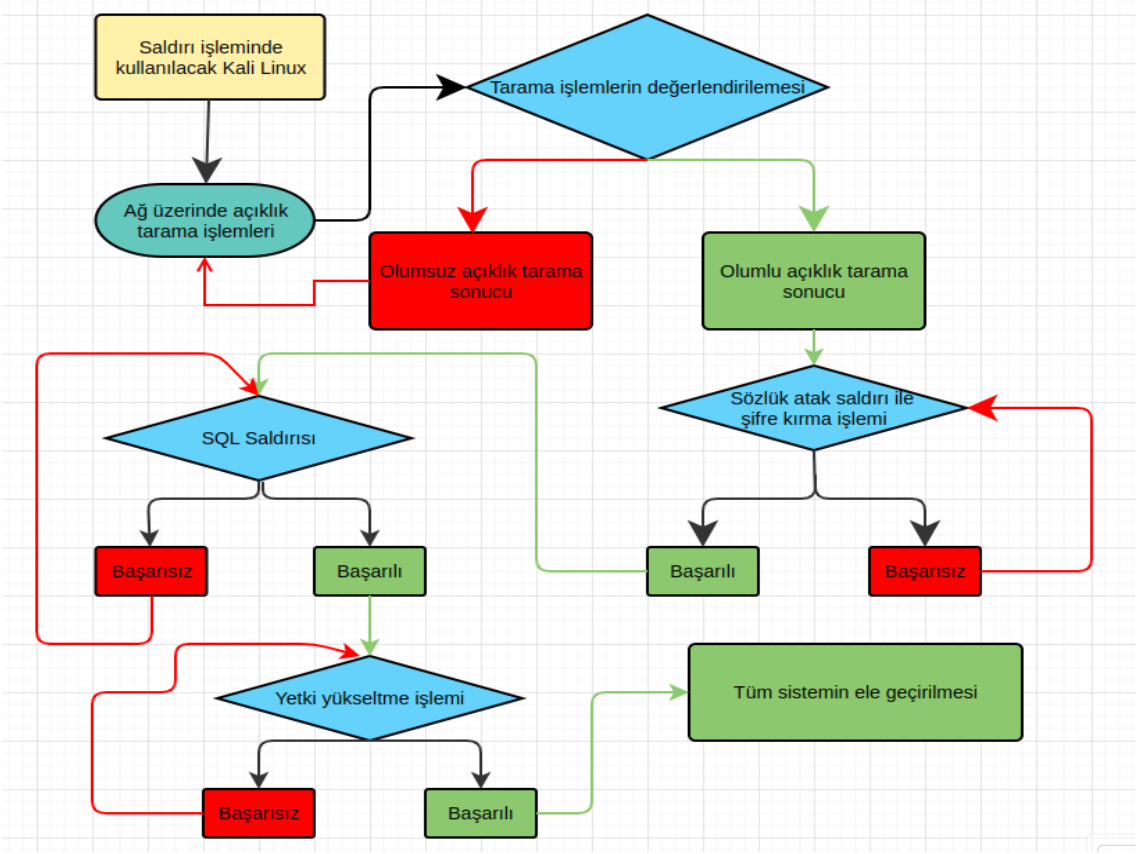
Çalışmada, beş ana konu temel alınmaktadır. Bunlar, (i) hedef sistemde açıklık barındıran bir web uygulaması tespit etmek, (ii) parola saldırısı ile admin (yönetici) parolasını ele geçirmek, (iii) SQL saldırısı ile hedef sistemde sistem komutları çalıştırabilmek, (iv) ters bağlantı ile hedef sisteme bağlantı sağlamak ve (v) yetki yükseltme ile sistemin ele geçirilmesi şeklindedir. Bütün bu aşamalar ve gerçekleştirilen saldırıların olay akış şeması Şekil 1'de blok diyagramı olarak verilmiştir.

Çalışmada temel alınan saldırılar aşağıdaki gibidir:

Açıklık Arama: Bağlı bulunulan ağ içerisinde herhangi bir açıklık barındıran bir web uygulaması tespit edilmeye çalışılmıştır. İlgili işlem için Kali Linux tarafından hazır gelen ağ taraması için kullanılan Netdiscover aracı komutu ile arama işlemi yapılmıştır. Ağ içerisinde tespit edilen bir IP Nmap aracı kullanılarak port taraması işlemi uygulanmıştır. Yapılan tarama işlemleri sonrası elde edilen bilgilerin internet yardımıyla herhangi bir açık barındırıp barındırmadığı kontrol edilmiştir.

Parola Saldırısı: Açıklık taramasında tespit edilen bir web sayfası admin girişine parola saldırısı gerçekleştirilerek parola kırma işlemi gerçekleştirilmiştir. Uygulanan işlem için Kali Linux tarafından hazır gelen CEWL (Cewl, 2024) ve John The Ripper (Ripper, 2024) araçları ile bir parola sözlüğü oluşturulup bu sözlük OWASP (OWASP, 2024) uygulaması ile kaba kuvvet uygulanarak web sayfası admin giriş parolası tespit edilmiştir.

SQL Saldırısı ve Ters Bağlantı Saldırısı: Saldırı kapsamında, admin sayfasına giriş yapabildiğimiz web sunucusu üzerinde PHP ve SQL enjeksiyonu yaparak sayfa üzerinde sistem komutlarını çalıştırması sağlanmıştır. İşlem sonrası bir adım öteye gidilerek ters bağlantı işlemi, MSFVenom aracı ile payload oluşturulup bunu Netcat üzerinden yüklenerek hedef sistem üzerinden bağlantı sağlanmıştır. Burada yapılan işlemler bir sonraki bölümde detaylı bir şekilde anlatılmıştır.



Şekil 1. Kali Linux ile hedef sisteme saldırı akış şeması

Yetki Yükseltme ve Sistemin Ele Geçirilmesi: Senaryoda, hedef sisteme bağlantı gerçekleştirildikten sonra bağlanılan sistemde yetki yükseltme işlemi (*local privilege escalation exploit*) açığı taraması yapılmaktadır. İşletim sistemine özgü bulunan açık Meterpreter aracı kullanılarak yetki yükseltme işlemi gerçekleştirilmekte ve hedef sistem ele geçirilmektedir.

Literatürde, bu konuyla ilgili birçok araştırma, makale ve kaynak bulunmaktadır. Kali Linux, açık kaynaklı bir Linux tabanlı işletim sistemidir ve içerisinde bir dizi sızma testi aracı barındırmaktadır. Kullanılan araçlar, ağ güvenliği açıklarını tespit etmek, zayıf noktaları

analiz etmek ve potansiyel saldırı senaryolarını değerlendirmek için kullanılmaktadır (Cisar ve Pinter, 2019; Kissi ve Asante, 2020).

Literatürdeki çalışmalar genellikle Kali Linux'in kullanımını, sızma testi adımlarını ve araçlarının yeteneklerini ve sızma testi sürecinin planlanması, hedef sistemlerin belirlenmesi, saldırı senaryolarının oluşturulması, güvenlik açıklıklarının keşfedilmesi ve raporlama gibi adımları kapsamaktadır. Yapılan çalışmalar, sızma testi sürecinin etik ve profesyonel bir şekilde yapılmasının önemini vurgulamakta ve güvenlik açıklıklarının tespit edilmesi ve giderilmesi için sızma testlerinin yaygın olarak kullanılması gerektiğini savunmaktadır (Gunawan ve ark., 2018a; Gunawan ve ark., 2018b). Ayrıca, gerçek dünya senaryolarında genellikle Kali Linux ve sızma testi araçlarının etkinliği ve verimliliği değerlendirmektedir. Bu çalışmalar, farklı ağ yapıları, web uygulamaları, sunucular ve mobil cihazlar gibi çeşitli hedef sistemler üzerinde sızma testi senaryoları gerçekleştirerek, güvenlik açıklıklarının ve zayıf noktaların tespit edilmesi konusunda önemli bir bilgi sağlamaktadır.

Sonuç olarak, Kali Linux ve kullanılan sızma araçları hakkında yapılan araştırmalar, bilgisayar güvenliği ve siber güvenlik alanında önemli bir yer tutmaktadır. Araştırmalar, sızma testi sürecinin önemini vurgulamakta, güvenlik açıklıklarının tespit edilmesi ve giderilmesi için bu tür araçların etkin kullanımını desteklemekte ve güvenlik uzmanlarına rehberlik etmektedir (Şentürk, 2018).

Çalışmamızda, üç farklı saldırı türü kullanılarak hedef sistem ele geçirilmektedir. Bunlar sırasıyla parola saldırısı, SQL saldırısı ve yetki yükseltme şeklinde gerçekleştirilmektedir.

Parola saldırısı, bir sistemde kullanılan parolaları keşfetmek veya çalmak amacıyla gerçekleştirilen bir saldırı türüdür. Literatürde parola saldırıları ve bunların önlenmesi üzerine çeşitli çalışmalar mevcuttur. Çalışmalar, güvenli şifreleme algoritmaları, parola karmaşıklığı politikaları ve güvenli kimlik doğrulama yöntemleri gibi konuları içermektedir (Lu ve Yu, 2021).

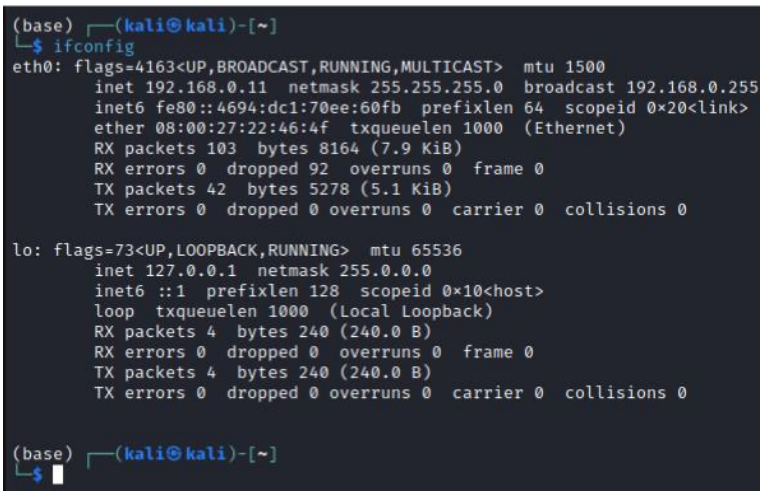
SQL saldırısı, kullanıcının girişlerini manipüle ederek veya kötü niyetli SQL ifadeleri kullanarak veritabanına yetkisiz erişim sağlamayı hedeflemektedir. SQL saldırıları, güvenlik açıklıklarının olduğu web uygulamalarında yaygın olarak görülmektedir. Saldırılar, veritabanı sistemlerinin zayıf doğrulama veya sorgu işleme mekanizmalarından yararlanmaktadır. Yetki yükseltme, bir sistemin veya uygulamanın güvenlik mekanizmalarındaki hatalardan veya zayıf yapılandırmalardan yararlanarak gerçekleştirilebilmektedir. Yetki yükseltme saldırıları, sistemin koruma mekanizmalarını aşarak yönetici veya root düzeyinde erişim elde etmeyi hedeflemektedir. Literatürde, yetki yükseltme saldırıları, güvenlik açıklıkları, ayrıcalık

ayrıştırması ve kullanıcı yetkilendirme konularında farklı çalışmalar bulunmaktadır (Vouteva, 2015).

Bu çalışma, parola saldırıları, SQL saldırıları ve yetki yükseltme gibi güvenlik açıklıklarına yönelik olarak Kali Linux ve sızma testi araçlarının kullanımını içermektedir. Bu konular üzerine birçok çalışma ve kaynak bulunmasına rağmen, çalışmamızda mevcut bilgi birikimini bir araya getirerek, Kali Linux'un benzer saldırılarda nasıl kullanılabileceği konusunda pratik bir bakış sunmaktadır.

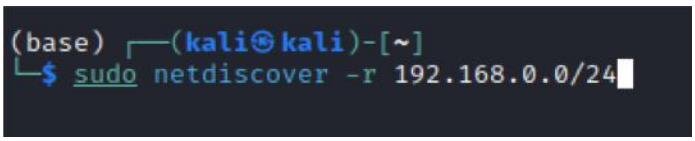
Deneysel Çalışmalar

Saldırı işlemleri sırasında sadece Kali Linux ve onunla birlikte gelen araçlar kullanılmıştır. Ağ içerisinde bir açıklık arama işlemine başlamadan önce Kali Linux'una ait makinenin IP adresinin tespit işlemi görülmektedir (Şekil-2).



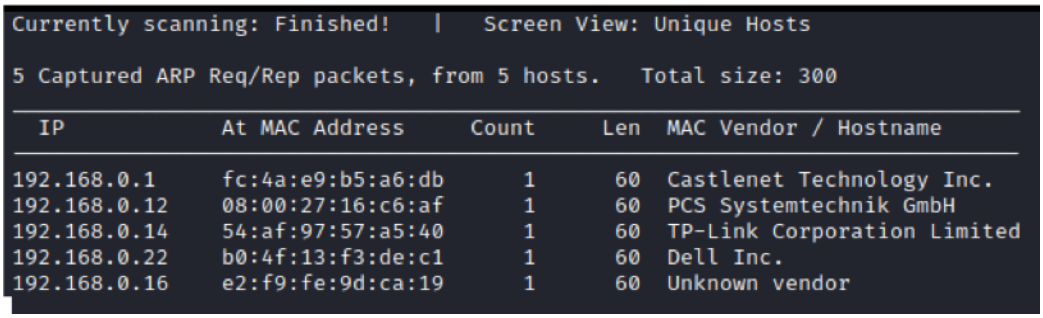
Şekil 2. Kali Linux IP tespiti

Elde edilen IP adresinden bulunan ağa ait tüm IP adreslerinin taramasının yapılacağı netdiscover komutu çalıştırılmıştır (Şekil-3).



Şekil 3. Netdiscover ile ağ tarama komutu

Bu tarama sonucunda ağ üzerinde bulunan aktif IP'ler tespit edilmiştir. Tespit edilen IP'ler sunulmaktadır (Şekil-4).

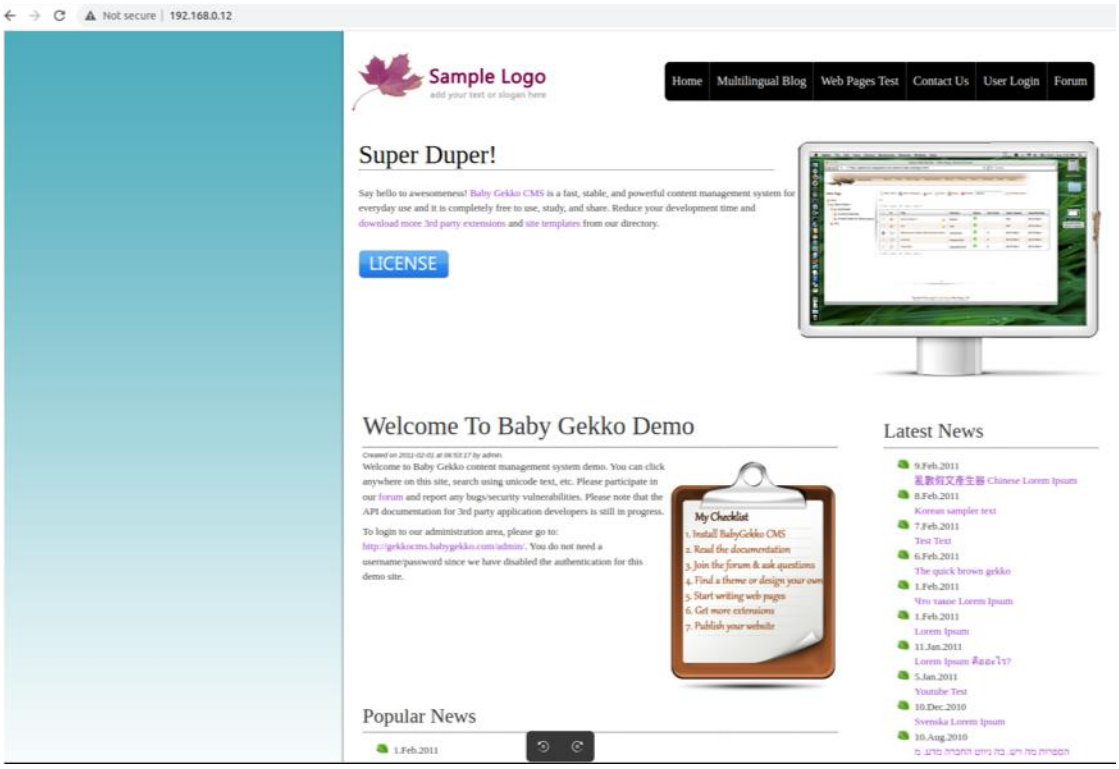


Şekil 4. Netdiscover ile ağ taraması sonuçları

Bir sonraki adım bu IP'ler üzerinde port araması yapılarak herhangi bir web sunucu olup olmadığını tespit etmektir. Bu işlem için Nmap aracı kullanılmıştır. Bu araç kullanımı ve elde edilen sonuç gösterilmektedir (Şekil-5).

Şekil 5. Nmap ile port taraması ve sonuçları

Tarama işlemi sonucunda ağ üzerinde 192.168.0.12 IP ile bir Baby Gekko isimli web sunucusu olduğu görülmektedir. Tespit edilen IP bir İnternet tarayıcı üzerinde açıldığında ön tanımlı kurulumda bırakılmış bir CMS uygulaması görülmektedir (Şekil-6).



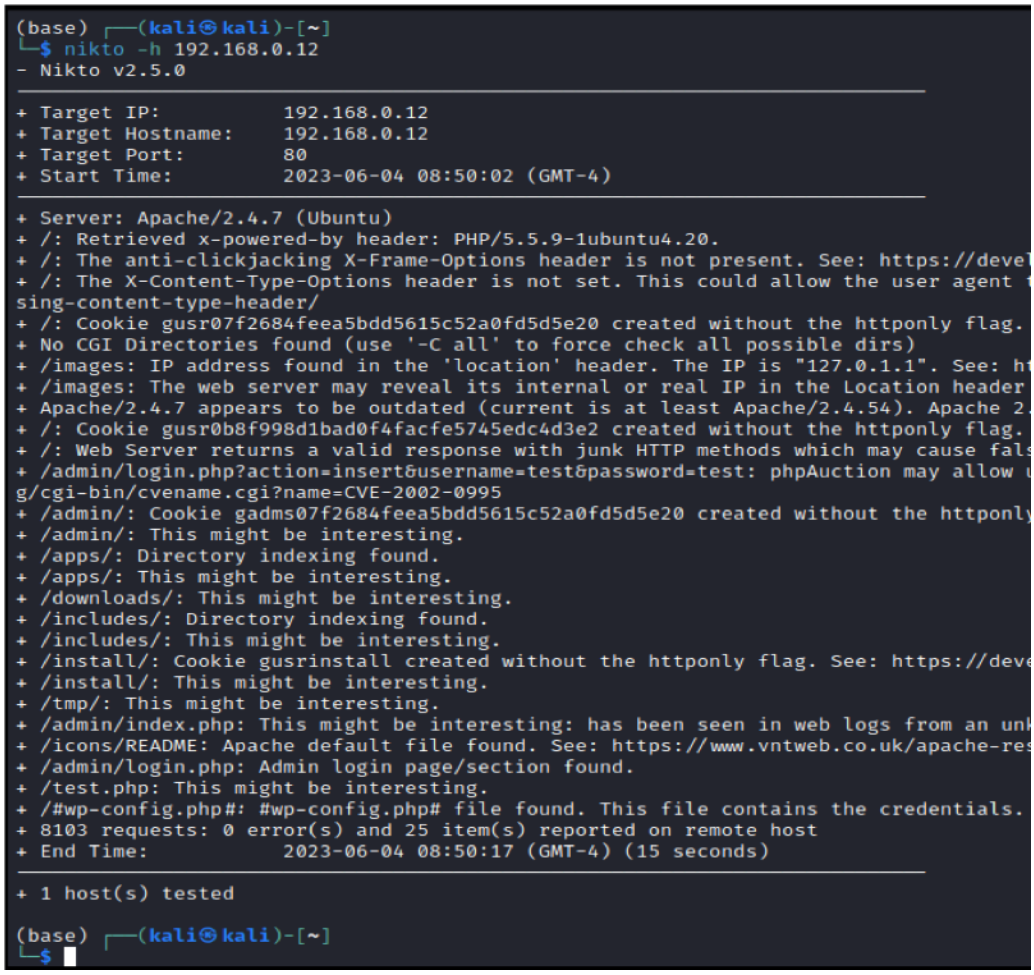
Şekil 6. CMS uygulaması

Tarama işlemi sonucu bulunan bu uygulamaya ait açıklıkların olup olmadığı Searchploit aracı ile aranmaktadır. Bu arama sonucuna göre ilgili uygulamaya ait güvenlik açıkları listelenmektedir (Şekil-7).

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit baby gekko
 Exploit Title
Baby Gekko CMS 1.1.5c - Multiple Persistent Cross-Site Scripting Vulnerabilities
BabyGekko 1.2.2e - Multiple Vulnerabilities
Shellcodes: No Results
```

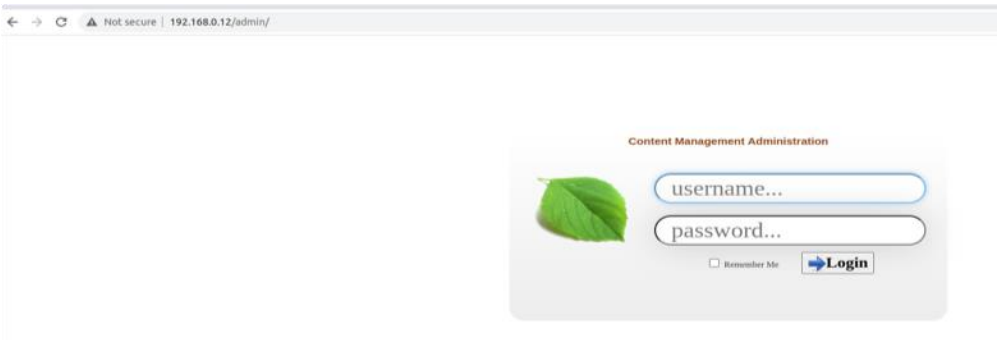
Şekil 7. Searchploit arama sonucu

Bir sonraki adımda Nikto uygulamasını kullanarak ilgili web sayfasına ait bir admin girişi bulunup bulunmadığının tespit edilmesi sağlanmıştır. Nikto uygulamasının sonucuna göre /admin link uzantısı ile bir admin giriş sayfası olduğu görülmektedir (Şekil-8).



Şekil 8. Nikto arama sonucu

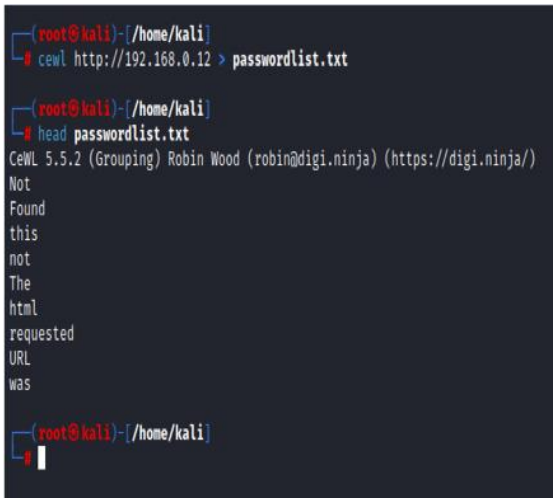
İlgili IP'nin devamında Nikto uygulaması ile bulunan admin link uzantısı eklenerek oluşturulan link web tarayıcısı üzerinden açılmaktadır. Link açıldığında Şekil 9'da sunulan admin sayfasına ulaşılmaktadır.



Şekil 9. Web sunucu admin sayfası

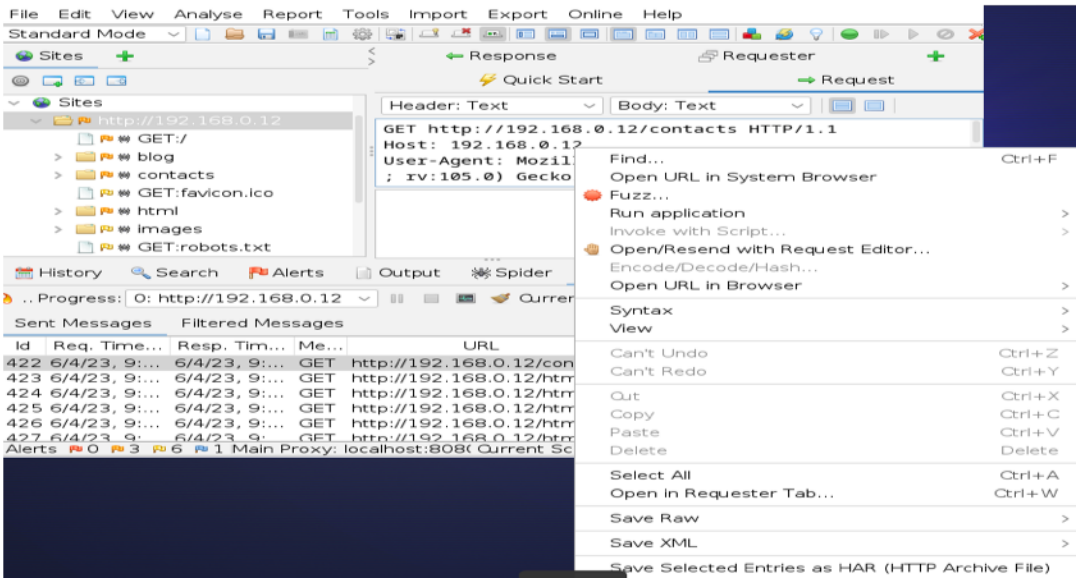
Admin sayfasına ulaşıldıktan sonra bir sonraki işlem olarak bu sayfayı Kali Linux'un sunduğu çeşitli parola saldırı araçlarını kullanarak parolayı ele geçirmektir. Yapılan işlemlerin

ilki için CEWL kullanılmıştır. Bu araç ilgili sayfadaki verileri kullanarak olası kelimelerden bir parola sözlüğü oluşturmaktadır. Sözlüğü genişletmek için John The Ripper uygulaması ile farklı algoritmalar kullanılarak olası parola ihtimalini arttırma işlemi gerçekleştirilmektedir. Araçlar ile oluşturulan parola listesi şekil üzerinde görülmektedir (Şekil-10).



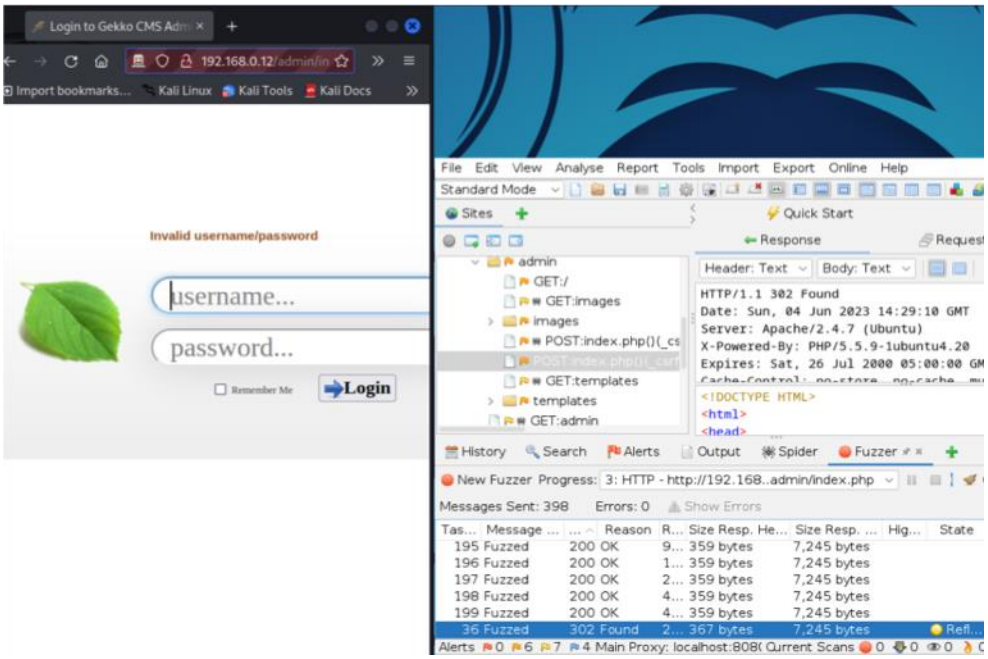
Şekil 10. CEWL ve John The Ripper uygulaması ile oluşturulan parola listesi

Parola listesini kullanabilmek için bir atak proxy kullanılması gerekmektedir. İşlem için Kali Linux'un sağladığı OWASP uygulaması kullanılmaktadır. Yapılan uygulama ile web sayfasının admin kısmına bağlanıldıktan sonra parola listesindeki parolaların teker teker denenmesi gerçekleştirilmektedir. OWASP uygulamasının hedeflenen web sayfasına bağlantısı gösterilmektedir (Şekil-11).



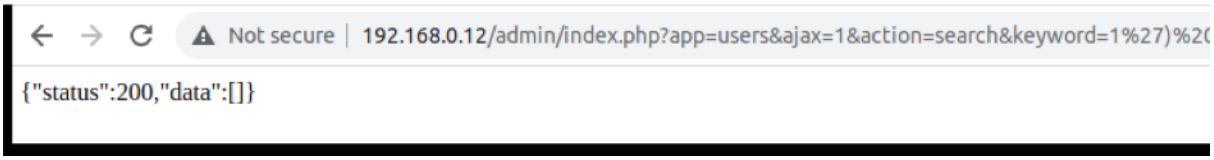
Şekil 11. OWASP ile hedef siteye bağlantının gerçekleştirilmesi

Uygulama üzerinden daha önce elde edilen parola listesi paylaşılarak admin sayfasında parolaların denenmesi otomatik olarak gerçekleştirilmektedir. Yapılan işlem sırasında; web sunucusundan doğru parola durumunda gönderilen "302 found" cevabı görülmektedir (Şekil-12). Böylelikle, admin sayfasının parolası elde edilmiş olmaktadır.



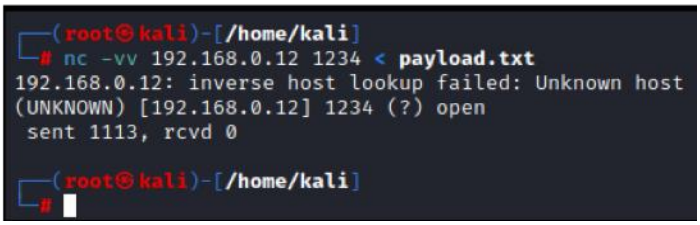
Şekil 12. OWASP ile hedef site admin parolasının tespiti

Gerçekleştirilen uygulama açık taraması işleminde bulunan açıklardan biri olan ve Şekil 6'da sunulan SQL enjeksiyon açığı, admin sayfasına erişim sağlandıktan sonra uygulanabilir bir duruma gelmektedir. İlgili SQL denemesi uygulandığında işlemin etkili olduğu görülmektedir (Şekil-13).



Şekil 13. Tarayıcı üzerinden yapılan test enjeksiyonu

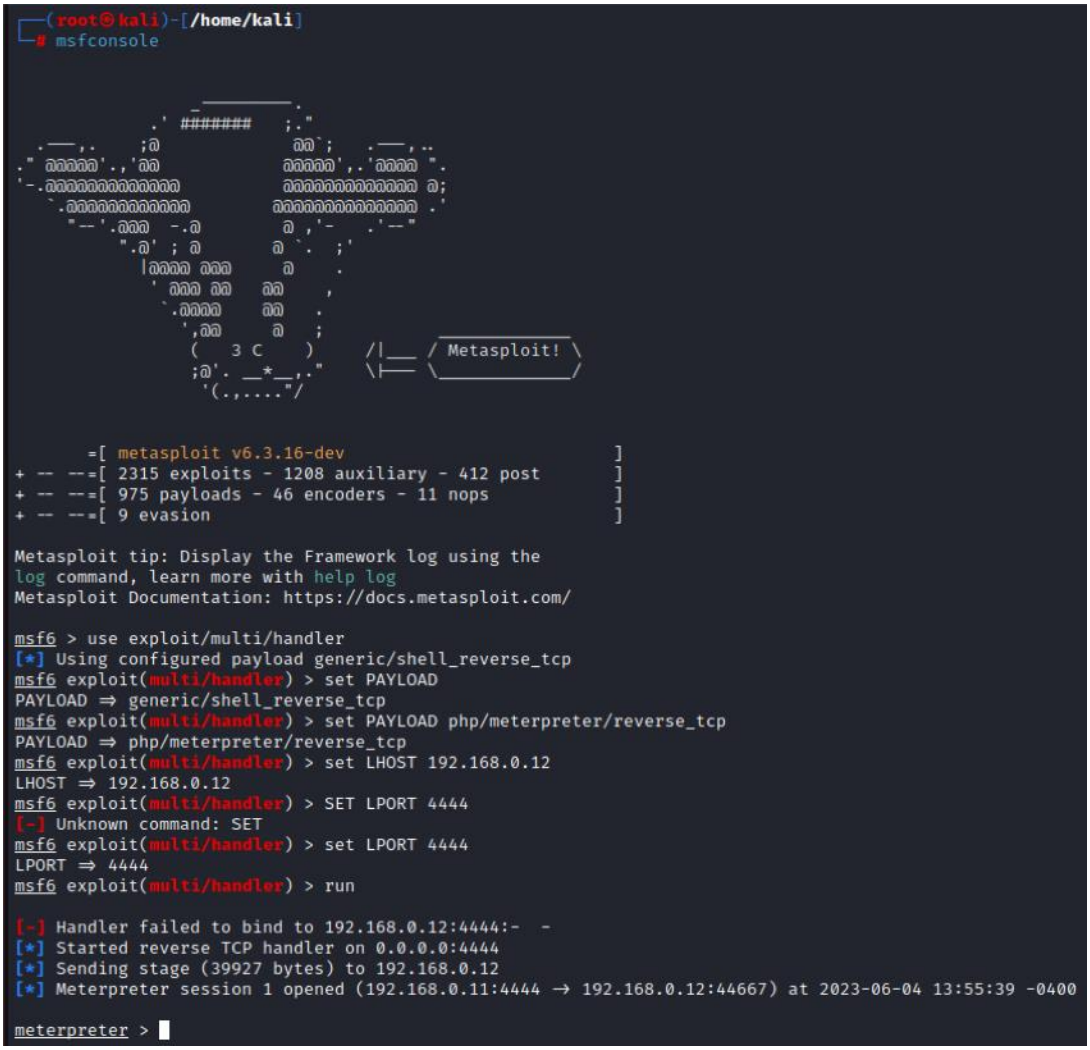
Böylelikle, web uygulaması üzerinde yapılan enjeksiyonun başarılı olduğu görülmektedir. Bir sonraki adım olarak web sunucu tarafından Netcat ile TCP portundan gelen veri dinlenmekte ve gelen veriyi reverse.php dosyasına aktaracak bir komut çalıştırılmaktadır. Sunucu üzerine yollanacak ters bağlantıyı sağlayacak PHP dosyası MSFVenom uygulaması ile oluşturulmaktadır (Şekil-14). Uygulanan işlemden sonra, saldırıyı gerçekleştiren bilgisayarda oluşturulan PHP payload'u hedef bilgisayara aktarılmaktadır.



Şekil 14. MSFVenom ile ters bağlantı PHP dosyası oluşturma

Ters bağlantı ile web sunucusu üzerinden atak bilgisayara bağlantı sağlanması amaçlanmaktadır. Oluşturulan reverse.php dosyasını sunucuya yükledikten sonra web tarayıcısı üzerinden 192.168.0.12/reverse.php komutu ile aktif edilmesi gerekmektedir. Böylelikle, ters bağlantı sunucu tarafından saldırı bilgisayarına doğru başlatılmaktadır.

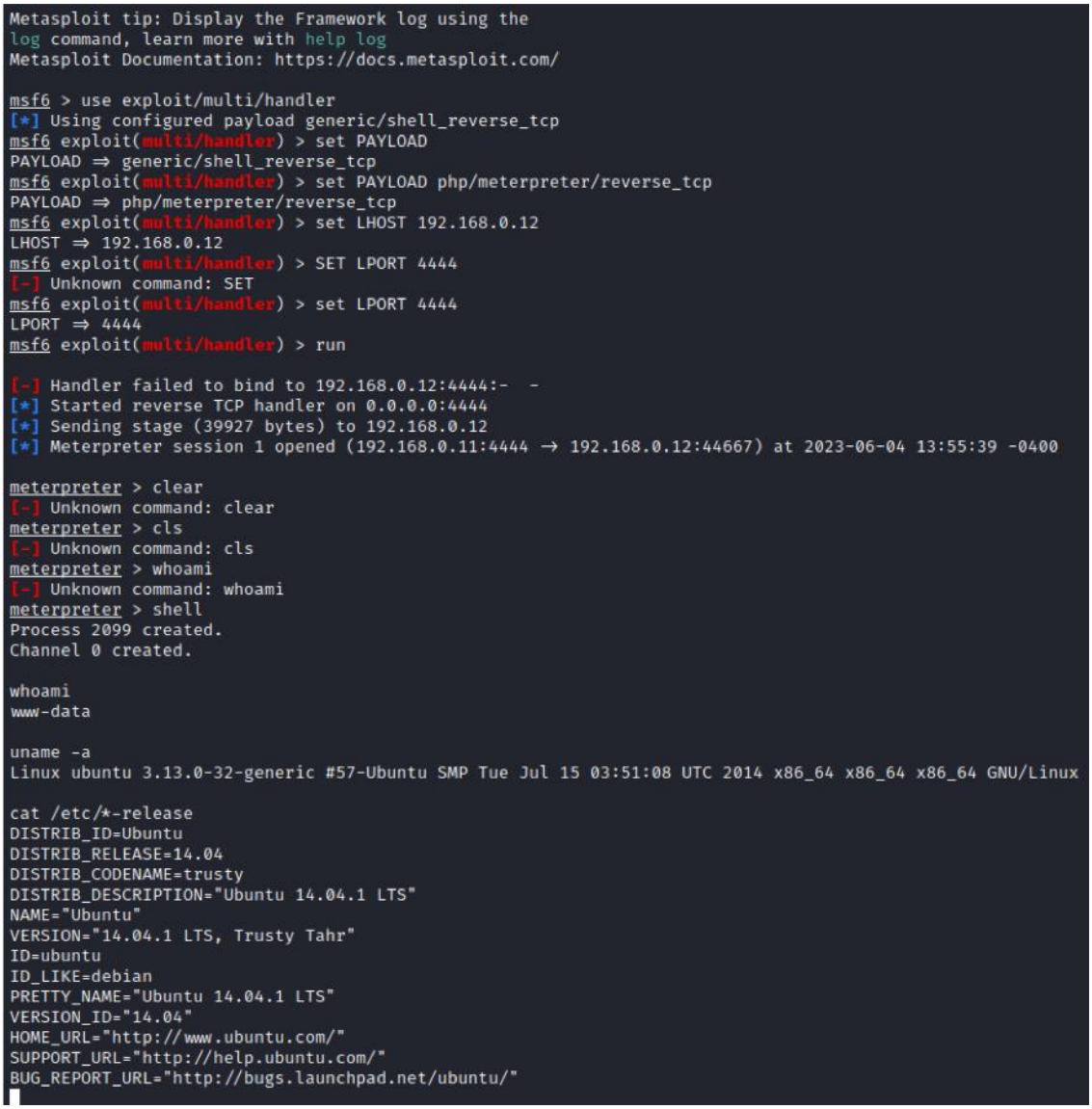
Atak yapılan bilgisayar tarafından Msfconsole uygulaması üzerinden bağlantı sağlanarak hedef bilgisayara bağlantı işlemi gerçekleştirilmektedir (Şekil-15).



Şekil 15. Msfconsole uygulaması ile sunucu bağlantısı (ters bağlantı yöntemi)

Bağlantı sağlandıktan sonra hedef sistem üzerinde gerekli değişiklikler yapılarak ele geçirme işlemi gerçekleştirilmektedir. Hedef sistemde yapılan bağlantıda root yetkili olarak bağlanıp bağlanılmadığı kontrol edilmektedir. Yapılan yetki sorgulamasında root yetkisine sahip olunmadığı Şekil 16'da gösterilmektedir.

Ters bağlantı sağlanan hedef sunucuda root yetkisi olmadığı durumlarda yapılacak işlemler kısıtlı olacağı için sağlanan bağlantının tam yetkili olması gerekmektedir. Tam yetkiyi ele geçirmek için hedef sistemin işletim sistemi hakkında bilgi edinilmeli ve yetki yükseltme işleminin gerçekleştirilmesi için kullanılan işletim sisteminin açıkları incelenmelidir.



Şekil 16. Metasploit üzerinde sunucu bağlantısı

Çalışmada hedef sistem olarak Kernel versiyonu Linux Ubuntu Kernel 3.13.0-32-generic olan Ubuntu 14.04 versiyonu kullanılmaktadır. Çalışmada uygulanan sistemde yetki

yükseltme için osf_64 uygulaması olduğu tespit edilmiştir. Uygulamamızda; Metasploit Meterpreter üzerinden yüklendiğinde root kullanıcısı olarak tam yetki sahibi olunabilmektedir. Uygulanan işlem sonrasında tüm hedef sistemi ele geçirilmiş olmaktadır. Böylelikle, tam yetkili olarak hedef sistem üzerinde her türlü değişikliği ve işlemi yapabilme kabiliyeti kazanılmaktadır.

Çalışma Sonucunda Elde Edilen Bulgular ve Tartışma

Kali Linux ve sızma testi araçlarının kullanımı, siber güvenlik alanında parola saldırıları, SQL saldırıları ve yetki yükseltme gibi güvenlik açıklıklarının tespiti ve önlenmesinde önemli bir rol oynamaktadır. Çalışmamızda, sızma testlerinin önemi ve bu testlerin düzgün bir şekilde gerçekleştirilmesinin kritikliği vurgulanmakta, Kali Linux ve sızma testi araçları kullanılarak sızma testi sürecinin temel adımları, ilgili adımların planlanma süreci ve hedeflenen sisteme yönelik saldırı senaryolarının gerçekleştirilmesi gösterilmektedir.

Sızma testlerinin etik kurallara uygun şekilde yapılması, hedeflenen sistemlere zarar vermek yerine güvenlik açıklıklarının ortaya çıkarılmasını hedeflemektedir. Çalışmamızda, sunulan deneysel gösterimler ve sızma testleri etik ve yasal konular dikkate alınarak yalnızca yasal izinler dahilinde ve hedef sistem sahibinin izniyle gerçekleştirilmelidir ve sunulan saldırı senaryoları ve kullanılan araçlar, sadece sızma testi amaçlı olarak belirlenen sistem üzerinde kullanılmalıdır. Ayrıca, sızma testlerinin sonuçları ve bulguları, hedef sistemin yönetici ve ilgili güvenlik ekipleriyle paylaşılmalıdır. Böylelikle, güvenlik açıklıkları tespit edilebilir ve gelecekteki saldırılara karşı etkili önlemlerin alınması sağlanabilir.

Sızma testlerine ek olarak; şifreleme, güvenlik duvarı kuralları, erişim kontrolleri ve diğer güvenlik önlemleri gibi önleyici güvenlik önlemlerinin de önemli olduğu unutulmamalıdır. Bu önlemler, potansiyel saldırıların engellenmesine ve sistemin güvenliğinin artırılmasına yardımcı olmaktadır (Altulaihan ve ark., 2023). Parola saldırıları, genellikle oturum açma bilgilerini ele geçirme veya yetkisiz erişim elde etme amacıyla ve Brute Force saldırıları, sözlük saldırıları, karma tablosu saldırıları gibi yöntemlerle gerçekleştirilmektedir.

Sonuç olarak, Kali Linux ve sızma testi araçlarının kullanımı siber güvenlik alanında çalışan uzmanlar için önemli bir yere sahiptir. Ancak, bu araçların dikkatli ve etik bir şekilde kullanılması gerekmektedir. Sızma testlerinin amacı, güvenlik açıklıklarını belirlemek ve sistemlerin güvenliğini artırmaktır. Sızma testlerinin yasal ve etik kurallara uygun olarak gerçekleştirilmesi ve sonuçların doğru şekilde değerlendirilmesi büyük önem taşımaktadır.

Sistem güvenliği, güncel ve güvenli yazılımların kullanılması, zayıf noktaların düzenli olarak tespit edilmesi ve uygun önlemlerin alınması ile sağlanabilir. Sızma testleri, sistemlerin güvenlik açıklarını belirlemek ve açıkları kapatmak için etkili bir yöntemdir. Böylelikle, sistem yöneticileri ve güvenlik uzmanları sistemlerindeki güvenlik açıklarını tespit edebilmekte ve gerekli önlemleri alarak sistemlerinin güvenliğini arttırabilmektedir.

Tablo 1. OWASP en önemli 10 web uygulaması güvenliği riskleri

Sıralama	Risk	Açıklama
1	Enjeksiyon (*Injection*)	Kötü niyetli kullanıcıların veri tabanına veya komuta girmesine izin veren hatalı giriş denetimi
2	Kırık Kimlik Doğrulama (*Broken Authentication*)	Kimlik doğrulama ve oturum yönetimi zafiyetleri
3	Hassas Veri Açığa Çıkarma (*Sensitive Data Exposure*)	Hassas verilerin gereksiz yere açığa çıkması veya korunmaması
4	XML Harici Varlık Saldırısı (*XML External Entity, XXE*)	Kötü amaçlı XML dokümanları kullanarak saldırı yapma yeteneği
5	Kırık Erişim Denetimi (*Broken Access Control*)	Kullanıcıların yetkilendirmeden kaçma veya yetkilerini yükseltme riski
6	Yanlış Güvenlik Yapılandırması (*Security Misconfiguration*)	Uygulama, sunucu veya veritabanı yanlış yapılandırıldığında ortaya çıkan riskler
7	Siteler Arası Betik Çalıştırma (*Cross-Site Scripting, XSS*)	Kötü niyetli kodların tarayıcılarda çalışmasına izin veren hatalı giriş denetimi
8	Güvensiz Serileştirme (*Insecure Deserialization*)	Serileştirme işleminin güvensiz kullanılması sonucu oluşan risk
9	Bilinen Güvenlik Açıkları Bulunan Bileşenlerin Kullanılması (*Using Components with Known Vulnerabilities*)	Güvenlik açıkları içeren üçüncü taraf bileşenlerin kullanılması
10	Yetersiz Günlükleme ve İzleme (*Insufficient Logging & Monitoring*)	Olayların ve hataların yeterince günlüklenmemesi veya izlenmemesi

Açık Web Uygulama Güvenliği Projesi (Open Web Application Security Project, OWASP) tarafından belirlenen 2017 yılındaki en önemli 10 web uygulaması güvenliği riskini içeren sıralama Tablo 1'de sunulmaktadır. Bu liste, web uygulamalarının güvenliği ile ilgili en büyük tehditleri sıralamaktadır. Yıllara göre güvenlik risk açıklarının sıralaması değişmekte ve listeye yeni yöntemler eklenmektedir. Örneğin, 2021 yılında Enjeksiyon (Injection) yöntemi üçüncü sıraya gerilerken Kırık Erişim Kontrolü (Broken Access Control) birinci sıraya gelmiştir. Çalışmamızda SQL saldırısı örneği uygulaması ile web

uygulamasındaki en büyük güvenlik açıklıklarından birinin uygulanması gösterilmiştir. Bu çalışmayla birlikte OWASP benzeri güvenlik açıklık listelerinin takip edilmesi ve bunlara sistemlerde önlem alınmasının önemi gösterilmektedir.

Çalışmamızın amacı, siber güvenlik alanında çalışmak isteyen araştırmacılar için bir kılavuz niteliğindedir. Çalışmada, Ubuntu 14.04 üzerinde Baby Gekko web sunucusu kullanılan bir hedef sisteme Kali Linux ve Kali Linux'te bulunan sızma testi araçları kullanılarak bir saldırı gerçekleştirilmiştir. Saldırı sürecinde, farklı araçlar ve teknikler kullanılarak hedef sisteme yetkisiz erişim sağlanmıştır. Çalışma kapsamında gerçekleştirilen deneysel saldırı sonucunda, hedef sistemde kullanılan sunucunun güvenlik açıkları tespit edilmiş ve zafiyetlerin saldırı olarak kullanılabileceği gösterilmiştir.

Sonuç olarak, yapılan çalışmada gerçekleştirilen saldırı örneği, siber güvenlik bilincini arttırmanın ve güvenlik önemlerini güçlendirmenin önemini göstermektedir. Çalışma ile alanda çalışmak isteyen araştırmacılara yönelik rehber bir kaynak sunulması hedeflenmiştir.

Sızma testleri, hedef sistemlerin güvenliğini sağlamak için önemlidir. Ancak, ilgili çalışmaların yasal ve etik kurallara uygun bir şekilde gerçekleştirilmesi gerektiği unutulmamalıdır. Sistem yöneticileri, güvenlik açıklarını tespit etmek ve düzeltmek için düzenli olarak sızma testlerin, yürütmeli ve güncel güvenlik önemlerini uygulamalıdır. Güvenlik açıklıkları, sürekli bulunan açıklıklar ve geliştirilen teknolojiler ile birlikte sürekli değişkenlik göstermektedir. Bu nedenle, risklerle başa çıkmak ve uygulamaları daha güvenli hale getirmek için gelecekteki çalışmalarımızda güncel OWASP riskleri ve bu riskleri gerçekleştiren çalışmalar yapılması planlanmaktadır.

Çıkar Çatışması Beyanı

Makale yazarları aralarında herhangi bir çıkar çatışması olmadığını beyan ederler.

Araştırmacıların Katkı Oranı Beyan Özeti

Yazarlar makaleye eşit oranda katkı sağlamış olduklarını beyan ederler.

Kaynaklar

Altulaihan EA, Alismail A, Frikha M., 2023. A Survey on web application penetration testing. Electronics, 12(5): 1229.

Cewl. https://www.kali.org/tools/cewl (Son Erişim: 01 Şubat, 2024).

Cisar P, Pinter R., 2019. Some ethical hacking possibilities in Kali Linux environment. Journal of Applied Technical and Educational Sciences, 9(4): 129-149.

Gunawan TS, Lim MK, Zulkurnain NF, Kartiwi M., 2018a. On the review and setup of security audit using Kali Linux. Indonesian Journal of Electrical Engineering and Computer Science, 11(1): 51-59.

Gunawan TS, Lim MK, Kartiwi M, Malik NA, Ismail N., 2018b. Penetration testing using kali linux: SQL injection, XSS, Wordpres, and WPA2 Attacks. Indonesian Journal of Electrical Engineering and Computer Science, 12(2): 729-737.

Kissi MK, Asante M., 2020. Penetration testing of IEEE 802.11 encryption protocols using Kali Linux Hacking Tools. International Journal of Computer Applications, 176: 32.

Lu HJ, Yu Y., 2021. Research on wiFi penetration testing with kali linux. Complexity, 2021: 5570001.

Ripper. John the Ripper password cracker. https://www.openwall.com/john (Son Erişim: 01 Şubat, 2024).

Şentürk MY., 2018. Güncel siber saldırı yöntemleri, sızma testi araçları ve temsili bir kurumsal ağ üzerinde uygulaması. Türk Hava Kurumu Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik ve Bilgisayar Mühendisliği Anabilim Dalı, s.16.

Vouteva S., 2015. Feasibility and deployment of bad USB. System and Network Engineering Master Research Project, University of Amsterdam, 1-17.

OWASP. OWASP Top 10 Vulnerabilities. https://owasp.org/www-project-top-ten (Son Erişim: 01 Şubat, 2024).