



Pyramid of Pain

İREM GÜZEL
15.02.2025

İçindekiler

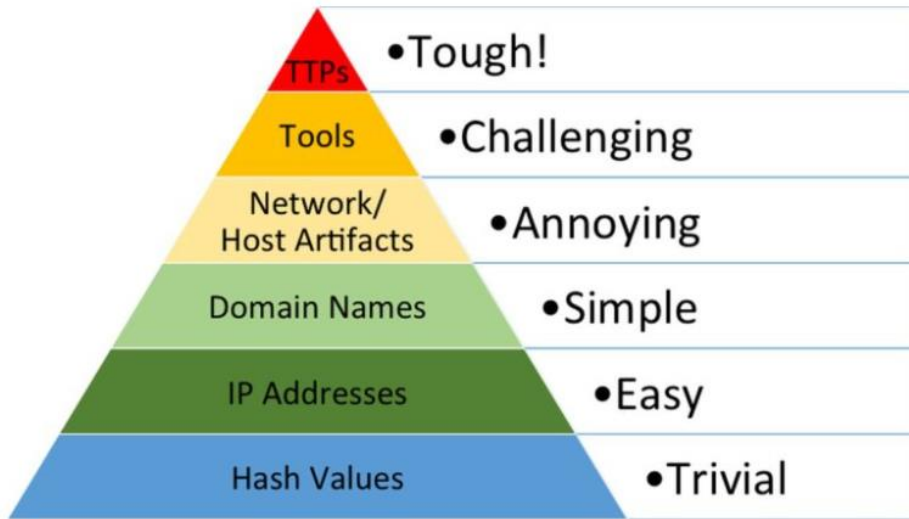
Giriş.....	3
Pyramid of Pain Nedir ?.....	3
1. Hash Values - Hash değerleri.....	4
2. IP Addresses - IP adresleri	5
3. Domain Names – Alan Adları.....	5
4. Host/Networks Artifacts - Ağ/Ana Bilgisayar Eserleri	5
5. Tools – Araçlar	6
6. TTP - Teknik, Taktik, Prosedürler.....	7
Sonuç.....	7
KAYNAKÇA	8

Giriş

Siber güvenlikte tehdit istihbaratı ve olay müdahalesi süreçleri, kuruluşların siber tehditlere karşı duruşlarını güçlendirmek için hayati öneme sahiptir. Bu süreçleri geliştirmek için çeşitli metodolojiler kullanılır ve Pyramid of Pain bu yaklaşımlardan biridir. David J. Bianco tarafından geliştirilen bu model, tehditlerin tespit edilmesi ve saldırganların operasyonlarının zorlaştırılması için güvenlik ekiplerine stratejik bir çerçeve sunar. Bu raporda, Pyramid of Pain'in bileşenleri ve ayrıntılı olarak incelenecektir.

Pyramid of Pain Nedir ?

Pyramid of Pain, farklı seviyelerdeki güvenlik önlemlerini hiyerarşik bir yapıda sunar. Piramidin alt seviyeleri temel güvenlik adımlarını, orta seviyeler daha ileri düzey önlemleri ve üst seviyeler ise en sofistike çözümleri içerir.



Piramidin en alt seviyeleri, temel siber güvenlik önlemlerini kapsar. Bu seviyede, ağ erişim kontrolü, güvenlik duvarları, antivirüs yazılımları, yama yönetimi ve güvenlik politikaları gibi temel koruma adımları bulunur.

Orta seviyede ise ağ güvenliği için daha gelişmiş önlemler yer alır. Bu aşamada, saldırı tespit ve önleme sistemleri, trafiğin şifrelenmesi, kimlik doğrulama ve yetkilendirme mekanizmaları ile güvenlik bilgisi ve olay yönetimi (SIEM) gibi çözümler devreye girer.

Piramidin en üst seviyesinde ise ileri düzey siber güvenlik stratejileri yer alır. Yapay zeka ve makine öğrenimi destekli güvenlik çözümleri, davranışsal analiz, siber tehdit istihbaratı, uçtan

uca şifreleme, güvenli yazılım geliştirme ve kapsamlı veri güvenliği gibi sofistike yaklaşımlar bu seviyede uygulanır.

Bu yapıya daha detaylı bakalım.

1. Hash Values - Hash değerleri

Hash değerleri, verilerin benzersiz bir özetini oluşturmak için kullanılan bir fonksiyon türüdür. Hash fonksiyonları, herhangi bir boyuttaki veriyi alır ve sabit uzunlukta bir dizeye dönüştürür. Bu dizeye "hash değeri" veya "parmak izi" denir.

Siber güvenlikte hash değerleri, zararlı yazılımların tespit edilmesi ve analiz edilmesi için de kullanılır. Her zararlı yazılımın kendine özgü bir hash değeri vardır. Bu sayede, bir zararlı yazılım tespit edildiğinde, hash değeri kullanılarak diğer sistemlerde de aynı zararlı yazılımın olup olmadığı kontrol edilebilir.

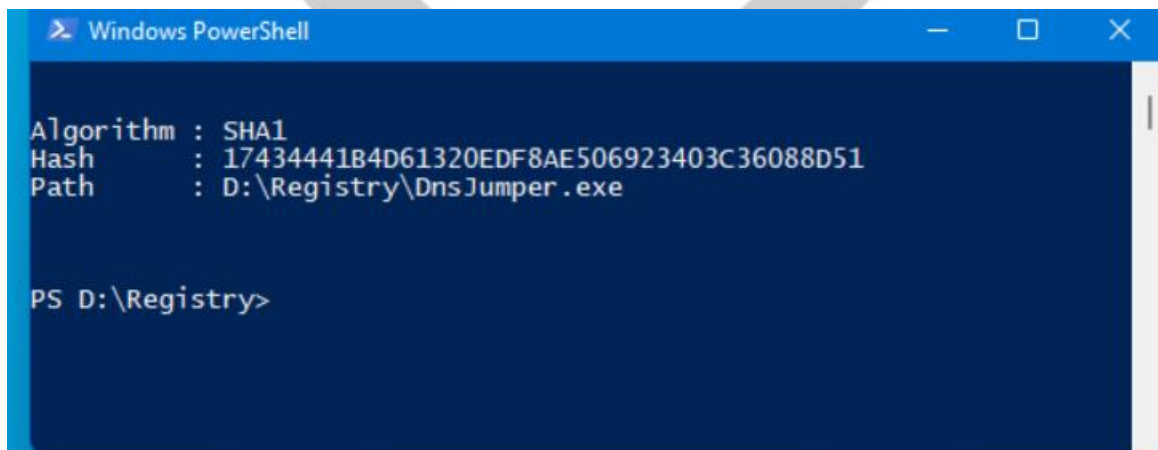
Hash değerlerini aramak için virustotal veya OPSWAT kullanılabilir.

Hash Değeri Kullanım Alanları

- Verinin bütünlüğünü doğrulama,
- Parolaları saklama,
- Sayısal imza,
- Mesaj doğrulama kodu
- Zararlı Yazılım Tespiti

Hash Algoritmaları:

- MD5
- SHA-1
- SHA-256
- SHA-384
- SHA-512



```
Windows PowerShell

Algorithm : SHA1
Hash      : 17434441B4D61320EDF8AE506923403C36088D51
Path      : D:\Registry\DnsJumper.exe

PS D:\Registry>
```

2. IP Addresses - IP adresleri

IP adresleri, internete bağılı cihazların (bilgisayarlar, sunucular, telefonlar vb.) internet üzerindeki adresleridir. Bu adresler cihazların birbirleriyle iletişim kurmasını sağlar. Saldırganlar, hedef sistemlere erişmek veya kötü amaçlı faaliyetlerini yürütmek için belirli IP adreslerini kullanırlar. Ancak IP adresleri, saldırıganlar tarafından kolayca değıştirilebilir. Bir saldırıgan, bir IP adresi engellendiğinde kolayca yeni bir IP adresi alabilir.

Bu nedenle, IP adresleri tek başına güvenilir bir saldırı belirtisi olarak kabul edilmezler.

3. Domain Names – Alan Adları

“Domain Names” Pyramid of Pain’in üçüncü seviyesinde yer alır

Web sitelerinin ve diğere internet servislerinin internet üzerindeki adreslerini ifade eder. Örneğın, "google.com" bir alan adıdır. Saldırganlar, kötü amaçlı web siteleri veya e-posta sunucuları için alan adları kullanabilirler.

Saldırganların kullandığı alan adlarını bilmek bizim için bir hazırlık olabilir. Ancak saldırıganlar, aynı IP adresleri gibi yeni alan adları alarak bu aşamayı da atlatabilirler.

4. Host/Networks Artifacts - Ağ/Ana Bilgisayar Eserleri

Piramidin dördüncü seviyesinde network/host artifacts yer alır.

Ağ/ana bilgisayar eserleri, bir saldırı sırasında veya sonrasında hedef sistemlerde ve ağlarda bırakılan izlerdir. Bunlar, saldırıganların kullandığı araçlar, oluşturduğu dosyalar, veya bıraktığı diğere kanıtlar olabilir.

Network Artifacts (Ağ Eserleri)

- IP Adresleri
- DNS Sorguları
- Ağ Trafiğı
- Portlar
- C2 Trafiğı
- ARP Zehirleme İzleri
- VPN ve Proxy Kullanımı
- Paket Yakalama Verileri (PCAP)

Host Artifacts (Ana Bilgisayar Eserleri)

- Log Kayıtları
- Kötü Amaçlı Yazılım İzleri
- Registry Değişiklikleri
- Yeni Kullanıcı Hesapları
- Yetki Yükseltme İzleri
- Şüpheli Süreçler
- Dosya Sistemindeki Anomaliler
- Bellek Dökümleri
- Zaman Damgalarıyla Oynama
- SSH Anahtarları ve Kimlik Bilgileri

Ağ/ana bilgisayar eserleri, bir önceki basamaklara göre manipüle edilmesi kısmen daha zordur. Bir saldırının detayları konusunda bize daha anlamlı bilgiler sunar. Aynı zamanda saldırının adımlarından yola çıkılarak saldırganların stratejisi çözülebilir ve savunma stratejileri de geliştirilebilir.

5. Tools – Araçlar

Piramidin beşinci seviyesinde **tools** yer alır.

Bu kısımda tehdit aktörlerinin hedeflerine ulaşmak için kullandığı yazılımlar, donanımlar veya teknikler tespit edilip analiz edilebilir.

Tools

- Kötü Amaçlı Yazılımlar
 - Virüsler
 - Casus Yazılımlar
 - Solucanlar
 - Botnetler
 - Truva Atları
- Saldırı Araçları
 - Exploit Kitleri
 - Parola Kırma Araçları
 - Kimlik Bilgisi Toplama Araçları
 - DDoS Saldırı Araçları
 - Kodlama ve Exploit Geliştirme Araçları
- Sosyal Mühendislik Teknikleri
 - Phishing : Sahte e-postalar vb sistemler ile kullanıcıları kandırarak kimlik bilgilerini ele geçirme yöntemidir.
 - Baiting (Yemleme) : İnsanları meraklandırıran veya cezbeden ücretsiz ürünler, çekilişler gibi taktiklerdir.

- Vishing (Sesli Oltalama) : Telefon veya sesli mesaj yoluyla insanları kandırarak hassas bilgilerini elde etme yöntemidir.
- Quid Pro Quo (Ver-Karşılık Al) : İnsanlara bir şey vererek (bilgi, hediye) karşılığında bir şey (hassas bilgi, erişim izni) alma yöntemidir.
- Tailgating (Kapıdan Takip Etme) : Kişiyi veya çalışanı takip ederek fiziksel alanına girmesidir.
- Pretexting : Bir senaryoda yetkili bir kimlik kullanarak insanları kandırarak bilgi elde etme yöntemidir.
- Whaling : Yüksek profilli kişileri hedef alan oltalama saldırılarıdır.

6. TTP - Teknik, Taktik, Prosedürler

Piramidin son seviyesinde TTP'ler yer alır.

TTP'ler Mitre Att&ck 'taki "Taktikler, Teknikler ve Prosedürler" anlamına gelir. Bir saldırganın hedefe saldırmak için kullandığı yöntemleri ifade eder.

Piramidin bu kısmı kırmızı renktedir çünkü bu aşamada saldırganın davranışları ile doğrudan kim olduğuna dair çıkarım yapılabilir. Bu bilgi ise saldırganın sonraki hamlelerini önceden bilmek ve ona göre karşı hamleler yapmayı sağlayarak kolayca saldırganı saf dışı bırakabilir.

Hacker gruplarının TTP'leri hakkında bilgi toplamak için MITRE ATT&CK kullanabilirsiniz.

Sonuç

Pyramid of Pain siber güvenlikte süreçleri optimize etmek için kritik bir çerçevedir. Her bir basamağın etkin bir şekilde anlaşılması ve ilgili işlemlerin uygulanması savunma açısından büyük bir yol haritası çizmektedir. Bu modelin etkin bir şekilde kullanılması, siber tehditlerle mücadelede önemli bir avantaj sağlayacaktır.

KAYNAKÇA

<https://medium.com/software-development-turkey/a%C4%9Fr%C4%B1-piramidi-pyramid-of-pain-91554269b9b6>

<https://sdogancesur.medium.com/a%C4%9Fr%C4%B1-piramidi-pyramid-of-pain-nedir-d20f3d86541e>

<https://www.attackiq.com/glossary/pyramid-of-pain/>

<https://chatgpt.com/>

