**Pyramid Of Pain**

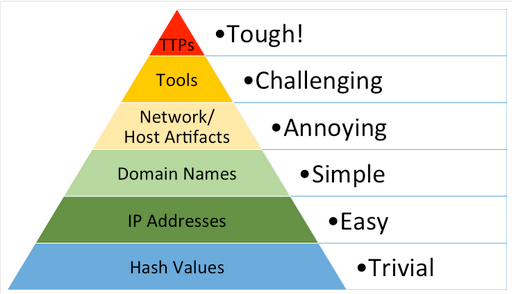
**•HAZIRLAYAN:**Sude SARIÇ

**•TARİH:**15.02.2024

**GİRİŞ:**Bu raporda Pyramid Of Pain hakkında detaylı bilgilere öğrenilip,siber güvenlik alanındaki yerini öğreneceğiz.

**Pyramid Of Pain**

Pyramid Of Pain, David Bianco tarafından geliştirilen, siber güvenlik savunmaları bağlamında bir saldırganın tespit edilmekten kaçınmak ve saldırısına devam etmek için karşılaşacağı zorluk seviyelerini ve maliyeti gösteren kavramsal bir çerçevedir.



Bu piramit, kurban makine kullanıcısının saldırganı fark etmesi sonrası, saldırgana karşı harekete geçerek yapılacak işlemlerin saldırgana ne kadar acı vereceğini anlatır. Yani burda acıdan kastımız saldırgana karşı koymanın, saldırganın amacına ulaşmasını engelleyerek saldırganı sinir küpüne çevirmek.

Pyramid of pain 6 seviyeden oluşuyor. Bu seviyeleri en alttan en üste (en az acı verenden, en fazla acı verene) sıralayalım.

1. **Hash Values**: Hash değeri, verileri benzersiz şekilde tanımlayan sayısal bir değeredir. hashing algoritması sonucu bir yazılımı veya dosyayı şifreleyerek benzersiz bir çıktı

elde eder. en yaygın hash algoritmaları MD5, SHA-1 ve SHA-2 algoritmalarıdır.

1. **IP Address**: Saldırının en yaygın göstergesi IP adreslerdir.
2. **Domain Names:** Bir web sitesinin IP, adresini sayısal olmayan bir isimle eşleştirir. Ulaşmak istediğimiz web sitesine veya sunucuya IP adresi kullanmadan giriş yapabilmemizi sağlar, ilgili IP adresine eşleştirilmiş bir isim mesela “medium.com” gibi, saldırganlar başka bir IP adresiyle mesela “medıum.com” eşleştirip punycode saldırısı gerçekleştirirler.
3. **Network/Host Artifacts**: Bir ağdaki kötü amaçlı işlemleri açıkça ayıran bir etkinliğin öğeleridir. Bu network/host yapıları command ve control (C2) bilgileri URL kalıpları, dizinler, dosyalar vb. biçiminde olabilir.
4. **Tools**: Saldırganların kötü amaçlı kodlar geliştirmek ve çalıştırmak, C2 oturumları başlatmak, parola kırmak, hata taramak için kullandıkları araçlardır. bu araçları saldırganların kullanmasını engellemek onlar için iyi olmaz ama güvenliğimiz için iyi olacaktır.
5. **TTP’s (Tactics, Techniques, and Procedures):** TTP’s,bir hacker metodolojisi olarak anlatılabilir. Tactics, (taktikler) bir saldırganın davranışını tanımlar. Techniques, (teknikler) saldırganın taktiklerine dayalı davranışını özetler. Procedures (prosedürler) de teknikleri gösterir.

**Neden Önemlidir?**

“Pyramid of Pain” modeli, siber güvenlik savunucularının (Blue Team) tehditleri sadece tespit etmekle kalmayıp, saldırganların taktik ve yöntemlerini değiştirmeye zorlayacak stratejiler geliştirmesini sağlar. Bu da siber saldırganlar için maliyeti ve zorluğu artırır, başarılı bir savunma stratejisi oluşturmak için önemli bir yapı taşıdır.

Bu modelle, saldırganları ne kadar zorlayabileceğinizi ve hangi noktada en çok “acı” verebileceğinizi anlamak, güçlü bir savunma inşa etmek için kritik önem taşır.

**SONUÇ:**

Bu rapor kapsamında Pyramid of Pain modeli katmanları,önemini detaylı bir şekilde işlemiş olduk.

**KAYNAKÇA:**

**<https://cybershieldcommunity.com/pyramid-of-pain/>**

**<https://medium.com/@davutenesersoz/pyramid-of-pain-nedir-763ae1d8ab79>**

**<https://www.sans.org/tools/the-pyramid-of-pain/>**

**<https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain>**