Sunum Konuşma Metni

APT Simülasyonu İçin Özel Zeek/Bro Betiği Geliştirme

Çağatay Üresin – Ağ Güvenliği ve Analizi

---

1. Giriş – Çalışmanın Amacı

Bu çalışmanın temel amacı, klasik imza tabanlı IDS sistemlerinin kaçırdığı modern saldırı tekniklerini davranışsal analizle tespit edebilen bir Zeek betiği geliştirmektir.
APT saldırıları genellikle iz bırakmayan, gizli çalışan ve davranışlarını sürekli değiştiren saldırılardır. Bu yüzden davranışsal tespit yaklaşımı zorunlu hale gelmiştir.
Ben de çalışmamda DNS tünelleme saldırısını örnek alarak, bu saldırıya ait davranışsal göstergeleri yakalayan özel bir tespit betiği geliştirdim.

---

2. APT – Advanced Persistent Threat

APT saldırıları kısa süreli değildir; çoğu zaman aylar boyunca sistemde fark edilmeden kalırlar.
Bu saldırılar TTP dediğimiz taktik, teknik ve prosedürlere dayanır.
En önemli özellikleri, geleneksel imza tabanlı IDS'lerden kolayca kaçabilmeleridir.
Bu nedenle APT'lerin tespitinde sadece imza değil, davranışsal analiz kullanmak kritik önem taşır.

---

3. Seçilen Saldırı Tekniği – DNS Tunneling

DNS, normalde alan adlarını IP adreslerine çevirmek için kullanılan meşru bir protokoldür.
DNS Tunneling tekniğinde saldırganlar, DNS sorgularının içine gizli veri gömerek bu protokolü bir tür "gizli tünel" gibi kullanırlar.

Genel olarak şu özelliklere sahiptir:

- Uzun ve rastgele karakterlerden oluşan alt alan adları
- Sık aralıklarla yapılan DNS sorguları (yüksek sorgu frekansı)
- TXT gibi veri taşımaya elverişli DNS kayıt tiplerinin yoğun kullanımı

Bu çalışmada kullandığım örnek saldırı, dnscat2 benzeri bir DNS tünelleme aracının ürettiği trafiği içermektedir.
Geliştirdiğim Zeek betiği de özellikle bu üç davranışsal özelliği hedef alacak şekilde tasarlanmıştır.

---

4. Davranışsal Tespit Yaklaşımı

İmza tabanlı sistemler yalnızca bilinen saldırıları tespit eder.
Modern saldırılar ise kendilerini gizlemek için protokolün doğal davranışını taklit eder, trafiği şifreler veya meşru protokoller içine gömer.
Davranışsal tespit modeli, protokolün normal akışını öğrenir ve bu akıştan sapmaları analiz eder.

Bu çalışmada geliştirdiğim Zeek betiği de tam olarak bu mantıkla çalışmaktadır: DNS trafiğindeki anormal davranışları tespit etmeye odaklanır.

---

5. Zeek Nedir?

Zeek bir saldırı tespit sistemi değil; ağ güvenliği izleme platformudur.
Signature odaklı değildir, tamamen event-driven yani olay tabanlı çalışır.
Her protokol için ayrı event'ler tetiklenir: `dns_request`, `http_request`, `ssl_established` vb.
Geliştirilen betikler bu event'lerin içine davranış analizi yerleştirir.
Bu özellik Zeek'i modern, imza bırakmayan APT saldırılarının tespitinde oldukça güçlü bir araç haline getirir.

---

6. Zeek Betik Yapısı ve Event Modeli

Zeek betikleri fonksiyonlardan değil, event handler'lardan oluşur.
Bir DNS isteği yapıldığında `dns_request` olayı tetiklenir ve bizim yazdığımız kod bu noktada çalışır.

Ayrıca:

- Global tablolar üzerinden durumsal analiz yapılabilir,
- Zaman pencereleri tanımlanabilir,
- Notice Framework sayesinde tespit edilen anormallikler alarm olarak üretilebilir.

APT tespitinde, bu **durum tutma (state)** ve **zaman penceresi** mantığı oldukça kritik rol oynar.

---

7. Geliştirilen Script'in Tasarımı

Çalışmada geliştirdiğim script, `DNS_Tunnel` isimli bir Zeek modülü olarak yazılmıştır ve yeni bir uyarı tipi tanımlar:

- `DNS_TUNNELING_DETECTED` adlı özel bir Notice tipi eklenmiştir.

Script'in temel hedefi, DNS tünelleme trafiğini üç farklı davranışsal gösterge üzerinden tespit etmektir:

1. **Normal dışı uzunlukta domain sorguları**
    - `LONG_DOMAIN_THRESHOLD = 50`
    - 50 karakterden uzun domain'ler, içinde veri taşınan tünel sorgularına işaret edebilir.
2. **TXT kayıt tipinin şüpheli kullanımı**
    - `qtype == 16` kontrolü ile TXT kayıtları yakalanır.
    - TXT kayıtları, DNS tünelleme araçlarında sıklıkla veri taşıma kanalı olarak kullanılır.
3. **Kısa zaman penceresinde abartılı sorgu sayısı (yüksek sorgu frekansı)**
    - `QUERY_THRESHOLD = 100`, `WINDOW = 10secs` olarak belirlenmiştir.
    - Aynı kaynak IP'den, kısa sürede 100'den fazla DNS isteği gelmesi şüpheli kabul edilir.

Script, `query_count` adlı global bir tablo tutarak her kaynak IP için sorgu sayısını izler ve bu üç metriğe göre `NOTICE` üretir.

---

8. Tespit Edilen Davranışsal Göstergeler

Bu betik, DNS tünelleme davranışını üç farklı açıdan gözlemler:

1. **[LONG DOMAIN] – Uzun Alan Adı Uyarıları**
    - `if ( |domain| > LONG_DOMAIN_THRESHOLD )` satırıyla çalışır.
    - dnscat2'nin oluşturduğu paketlerde, alt alan adı kısmına gömülen şifreli/veri içeren stringler normal domainlere göre oldukça uzundur.
    - Test edilen PCAP üzerinde, bu uyarılar genellikle tünel trafiğine ait sorgular üzerinde yoğunlaşmıştır.
2. **[TXT QUERY] – TXT Kayıt Tipi Üzerinden Veri Taşıma**
    - `if ( qtype == 16 )` ile TXT sorguları tespit edilir.
    - DNS tünelleme araçları, metin verisini veya şifreli blokları TXT kayıtları içinde taşımayı sever.
    - dnscat2 PCAP'i üzerinde TXT sorguları neredeyse tamamen saldırı trafiğini temsil ettiği için, bu uyarı tipi yüksek doğrulukla sonuç vermiştir.
3. **[HIGH QUERY RATE] – Yüksek Sorgu Oranı**
    - `if ( query_count[src] > QUERY_THRESHOLD )` koşulu, belirli bir IP'nin kısa sürede anormal sayıda DNS sorgusu yaptığını gösterir.
    - Normal bir istemci tipik olarak bu kadar agresif DNS sorgusu üretmez.
    - dnscat2 PCAP'inde, tünel kuran istemci IP'si bu eşiği aşarak düzenli olarak C2 iletişimi kurduğu için, script tarafından işaretlenmiştir.

Bu üç uyarı türü bir araya geldiğinde, özellikle "uzun domain + TXT sorgusu + yüksek sorgu frekansı" kombinasyonu, DNS tünelleme faaliyetini oldukça net bir şekilde ortaya çıkarmaktadır.

---

9. Kullanılan Test PCAP'i

Testlerde, DNS tünelleme saldırısı içeren bir PCAP dosyası kullanılmıştır:

- PCAP Kaynağı: `dnscat2_dns_tunneling_24hr.pcap`
- Link: https://www.dropbox.com/s/4r9mcn792dbzonf/dnscat2_dns_tunneling_24hr.pcap?dl=0

Bu PCAP içerisinde:

- Uzun süreli bir DNS tünelleme oturumu,
- Sürekli ve düzenli aralıklarla yapılan DNS sorguları,
- TXT tipi DNS kayıtları üzerinden veri taşınması bulunmaktadır.

Zeek, Docker üzerinde çalıştırılmış ve bu PCAP offline modda analiz edilmiştir.
Sonuçlar `dns.log` ve `notice.log` dosyaları üzerinden incelenmiştir.

---

10. Uygulama Ortamı (Docker + Zeek)

Çalışmayı Security Onion yerine Docker üzerinde yaptım.

Bu yaklaşımın avantajları:

- Daha hızlı test döngüsü
- İzole bir analiz ortamı
- Script üzerinde küçük değişikliklerin kolay test edilebilmesi

PCAP, Zeek üzerinde offline/pcap analizi ile çalıştırılmıştır. Betik `dns_tunnel.zeek` adıyla yüklenmiş, üretilen alarmlar `notice.log` dosyasında toplanmıştır.

---

11. Test Sonuçları

Geliştirilen betik, `dnscat2_dns_tunneling_24hr.pcap` üzerinde çalıştırıldığında üç tip alarm üretmiştir:

1. **[LONG DOMAIN] Uyarıları**
    - Uzun ve rastgele görünen domain sorguları için tetiklenmiştir.
    - Bu uyarıların büyük çoğunluğu, tünel trafiğine ait sorgular üzerinde yoğunlaşmıştır.
2. **[TXT QUERY] Uyarıları**
    - TXT tipi DNS sorgularının neredeyse tamamı, tünel aracı tarafından üretilen trafiğe aittir.
    - Bu nedenle bu uyarı tipi, test senaryosunda yüksek doğruluk (yüksek true positive oranı) sağlamıştır.
3. **[HIGH QUERY RATE] Uyarıları**
    - Aynı kaynak IP'den kısa sürede çok sayıda sorgu geldiğinde tetiklenmiştir.
    - dnscat2'nin C2 iletişimi kurmaya çalışan istemcisi, bu eşiği aşarak düzenli olarak alarm üretmiştir.

Genel değerlendirme:

- Üç heuristik birlikte ele alındığında, DNS tünelleme trafiği başarıyla işaretlenmiştir.
- Test senaryosunda false-positive oranı oldukça düşüktür; çünkü hem uzun domain uzunlukları hem TXT tipi hem de yüksek sorgu oranı genellikle aynı saldırgan IP üzerinde toplanmıştır.
- Bu da scriptin, klasik imza gerektirmeden, tamamen davranışsal olarak saldırıyı tespit edebildiğini göstermektedir.

---

12. Performans Değerlendirmesi

Zeek oldukça optimize bir altyapıya sahip olduğu için script neredeyse sıfır ek yük oluşturmuştur.

Testlerde gözlemlenen genel durum:

- CPU kullanımının düşük seviyede kalması
- Bellek kullanımının stabil seyretmesi
- DNS event'lerinin gerçek zamanlı takibinde belirgin bir gecikme yaşanmaması

Script, yalnızca DNS event'leri üzerinde basit sayma ve uzunluk kontrolü yaptığı için karmaşık bir hesaplama yükü oluşturmamaktadır.
Bu da, gerçek ortamda daha yüksek trafik hacimlerinde bile çalışabilecek hafif bir davranışsal tespit mekanizması sunduğunu göstermektedir.

---

13. Sonuçlar ve Gelecek Çalışmalar

Geliştirilen script, DNS tünelleme saldırılarını davranışsal olarak başarılı şekilde tespit etmektedir.
İmza kullanmadan, yalnızca trafik özelliklerine bakarak tespit yapmak, APT türü saldırılara karşı önemli bir avantaj sağlar.

Bu yapı kolayca:

- HTTP, HTTPS/TLS veya diğer protokollere
- Farklı kayıt tiplerine (örneğin MX, CNAME anormallikleri) genişletilebilir.

Gelecek çalışmalar arasında:

- Makine öğrenmesi tabanlı anomali tespit modelleri ile eşik değerlerinin dinamik hale getirilmesi,
- SumStats framework kullanılarak daha esnek ve doğru zaman penceresi hesaplamaları yapılması gibi iyileştirmeler planlanabilir.

Bu da APT tespit kabiliyetini bir adım daha ileri götürebilir.

---

14. Soru & Cevap

Sunum burada sona ermektedir. Sorularınızı alabilirim.