BÜRKÜT-Güvenlik Güncellemeleri

BÜRKÜT PROJESİ: GÜVENLİK MİMARİSİ GÜNCELLEME PAKETİ (v2.0)

Gerekçe: "Layer 2/3 Black Hole" ve "Prompt Hijacking/Injection" saldırılarına karşı İç Ağ (LAN) güvenliğinin sıkılaştırılması.

1. Uygulama Katmanı: Kriptografik Mühür (HMAC Entegrasyonu)

- **Mevcut Durum:** Python Middleware scripti sadece IP kontrolü yapıyordu.
- **Alınan Karar:** İstemci (Operatör) ve Sunucu (AI Ajanı) arasına **HMAC-SHA256** imzalama mekanizması eklenecek.
- **Teknik Aksiyon:**
  - Operatörden giden her prompt, gizli bir anahtar (Secret Key) ile hash'lenecek.
  - Middleware, imzası geçersiz (değiştirilmiş/manipüle edilmiş) paketleri işleme almadan reddedecek (Drop).
- **Kazanım:** Saldırgan trafiği dinlese bile ("Man-in-the-Middle"), prompt içeriğini değiştiremez. Veri bütünlüğü (Integrity) sağlanır.

2. Sistem Katmanı: Kısıtlı Yetki (Gulam/Hizmetkar Modeli)

- **Mevcut Durum:** AI ajanı ve scriptlerin çalışma yetkileri standart kullanıcı seviyesindeydi.
- **Alınan Karar:** "En Az Yetki" (Least Privilege) prensibi uygulanacak.
- **Teknik Aksiyon:**
  - `ai_agent` isminde, `sudo` yetkisi olmayan izole bir kullanıcı oluşturulacak.
  - AI kaynak kodlarının sahibi (Owner) `root` olacak, `ai_agent` sadece "Okuma/Çalıştırma" (Read-Only/Exec) hakkına sahip olacak.
- **Kazanım:** AI hacklense veya halüsinasyon görse bile, kendi kaynak koduna "backdoor" gömemez veya sistem dosyalarını silemez.

3. Ağ Katmanı: L2 Gözetim ve ARP Bekçiliği

- **Mevcut Durum:** Wazuh sadece logları ve dosya bütünlüğünü izliyordu.
- **Alınan Karar:** Wazuh, OSI Katman 2 (Data Link) seviyesindeki anormallikleri de izleyecek.
- **Teknik Aksiyon:**
  - Wazuh Agent (Kali/Ubuntu) üzerine, Gateway (pfSense) MAC adresini periyodik kontrol eden (`arp -n`) bir script tanımlanacak.

    - Wazuh Manager'da, MAC adresi değişimini "Level 12 (Yüksek Risk)" olarak işaretleyen özel bir **XML Kuralı (Custom Rule)** yazılacak.
- **Kazanım:** Saldırganın sessizce yaptığı "ARP Spoofing" veya "Black Hole" girişimi, anında yüksek seviyeli bir güvenlik alarmına dönüşür.

4. Otonom Savunma: Aktif İzolasyon (Active Response)

- **Mevcut Durum:** Active Response mekanizması Brute Force ve Web saldırılarına odaklıydı.
- **Alınan Karar:** ARP Zehirlenmesi tespit edildiği an saldırgan ağdan düşürülecek.
- **Teknik Aksiyon:**
    - ARP Spoofing alarmı (Rule ID: 100050), `firewall-drop` komutunu tetikleyecek şekilde yapılandırılacak.
    - Saldırganın IP adresi `iptables` DROP listesine alınarak makine ile iletişimi çekirdek seviyesinde kesilecek.
- **Kazanım:** Saldırgan manipülasyon yapmaya fırsat bulamadan sistemden izole edilir (Detection to Prevention).