BÜRKÜT-Teknik Altyapı ve Hedefimiz

Teknik Altyapı ve Hedefimiz (Basitleştirilmiş):

1. **Ağ Geçidi ve İzolasyon (Yeni):** Laboratuvar trafiğini denetlemek ve dış dünyadan izole etmek için merkeze bir **pfSense Firewall** konumlandırılacak.
2. **Kurban Makine (Target):** Eski Metasploitable imajları yerine; ağın Host-Only (izole) bacağında çalışan "Modern Ubuntu Server (22.04 veya 24.04)" kurulacak.
3. **Zafiyet Motoru:** Zafiyetli uygulamalar doğrudan işletim sistemine değil, modern standartlara uygun olarak **Docker Konteynerleri** (örn: DVWA, Juice Shop, Log4j vb.) şeklinde ayağa kaldırılacak.
4. **Saldırgan Makine:** Kali Linux.
5. **Gözetleme ve Savunma:** Wazuh SIEM kullanılarak loglar toplanacak ve Active Response ile saldırılar otonom olarak engellenecek.
6. **Sanallaştırma Platformu:** Kararlılık ve performans avantajları nedeniyle **VMware Workstation Pro** kullanılacak.

Teknik Altyapı ve Hedefimiz (Geliştirilmiş):

1. **Sanallaştırma ve Kurumsal DMZ Mimarisi:** Kararlılık ve "Golden Snapshot" yetenekleri için **VMware Workstation Pro** kullanılacak. Sistem karmaşık çift-bacaklı (Dual-NIC) yapılardan arındırılarak, ağın merkezine donanımsal izolasyon ve kurumsal DMZ mantığı sağlayan bir **pfSense Firewall VM** yerleştirilecek. Böylece AI ajanının bulut API'lerine çıkışı kontrollü sağlanırken, fiziksel ağlara sızması L3/L4 seviyesinde engellenecektir.
2. **Kurban Makine (Target):** Sadece izole (Host-Only) ağa bağlı, pfSense üzerinden dış dünyaya (WAN) çıkışı kesinlikle kısıtlanmış (Strict Egress) **Modern Ubuntu Server (22.04/24.04)** kurulacak. Sistem üzerinde, tüm hareketleri gözetleme kulesine anlık aktaran SIEM ajanı barınacak.
3. **Zafiyet Motoru:** Zafiyetler doğrudan işletim sistemine değil, modern mikroservis standartlarına uygun olarak ve gerçek dünya zafiyetlerini (CVE) barındıran **Vulhub** reposu üzerinden **Docker Konteynerleri** şeklinde ayağa kaldırılacak.
4. **Saldırgan Makine (Attacker & AI Host): Kali Linux**. Üzerinde hem manuel sızma araçları hem de bulut tabanlı zekayı kullanan **AI Ajanı (MCP)** çalışacak. Yapay zekanın "halüsinasyon" görüp izole ağ dışına çıkmasını önlemek için Python (Middleware) ve iptables (Hard Kill Switch) tabanlı ek **Güvenlik Kilitleri (Guardrails)** uygulanacak.
5. **Gözetleme Kulesi ve Otonom Savunma (SIEM):** Laboratuvara entegre edilen üçüncü sanal makine olarak **Wazuh Manager** kullanılacak. Saldırı anında Active Response (Otonom Savunma) mekanizması tetiklenecek; ancak başarısı sadece bağlantı kopmasıyla

değil; **Wazuh Logları, Firewall State (Durum) Değişimi ve Servis Sağlığı (Masum Trafik Testi)** olmak üzere 3 farklı metrikle çapraz doğrulanacaktır.

6. **Hardening ve DevSecOps:** Bulunan zafiyetler öncelikle manuel müdahale ile tecrübe edilecek, sistem anatomisi kavrandıktan sonra "Infrastructure as Code" (IaC) felsefesiyle (Bash/Ansible) otomatize edilmiş operasyonlarla kalıcı olarak yamalanacaktır.
7. **AI Kalite Kontrol (QA) ve Metrikler:** Yapay zekadan yama scriptleri (IaC) önerisi istenecek ve yamalanan sistemin son durumu yine AI tarafından test edilecektir. Yapay zekanın bu süreçteki başarısı; **Müdahale Süresi, False-Positive (Yanlış Alarm) Oranı, Tutarlılık ve Güven Skoru (Confidence Scoring)** gibi kurumsal KPI'lar (Performans Göstergeleri) üzerinden raporlanacaktır.