# BÜRKÜT-Teknik Altyapı ve Hedefimiz

**Teknik Altyapı ve Hedefimiz(Basit):**

1. **Kurban Makine (Target):** Eski Metasploitable imajları yerine; "Modern Ubuntu Server (22.04 veya 24.04)" kurulacak.
2. **Zafiyet Motoru:** Zafiyetli uygulamalar doğrudan işletim sistemine değil, modern standartlara uygun olarak **Docker Konteynerleri** (örn: DVWA, Juice Shop, Log4j zafiyetli app vb.) şeklinde ayağa kaldırılacak.
3. **Saldırgan Makine:** Kali Linux.
4. **Sanallaştırma Platformu:** Kararlılık ve performans avantajları nedeniyle **VMware Workstation Pro** kullanılacak.
5. **Ağ Yapısı:** VMware üzerinde makinelerin birbiriyle konuştuğu ancak dış dünyadan izole edildiği güvenli bir yapı (NAT Network / Host-Only veya LAN Segment) kurulacak

**Teknik Altyapı ve Hedefimiz(Geliştirilmiş):**

1. **Sanallaştırma ve Ağ Mimarisi (Hibrit Topoloji):** Kararlılık ve "Golden Snapshot" yetenekleri için **VMware Workstation Pro** kullanılacak. Sistem geleneksel tam izole yapıdan çıkarılarak, **"Çift Bacaklı" (Dual-NIC)** hibrit bir ağ topolojisine (VMnet0 NAT ve VMnet2 Host-Only) geçirilecek. Böylece yapay zekanın bulut API'larına erişimine izin verilirken, kurban makinenin fiziksel ve dış ağlardan mutlak izolasyonu sağlanacak.
2. **Kurban Makine (Target):** Eski Metasploitable imajları yerine; sadece izole (Host-Only) ağa bağlı, dış dünyadan koparılmış **Modern Ubuntu Server (22.04 veya 24.04)** kurulacak. Sistem üzerinde, tüm hareketleri gözetleme kulesine anlık aktaran SIEM ajanı barınacak.
3. **Zafiyet Motoru:** Zafiyetli uygulamalar doğrudan işletim sistemine değil, modern mikroservis standartlarına uygun olarak ve gerçek dünya zafiyetlerini (CVE) barındıran **Vulhub** reposu üzerinden **Docker Konteynerleri** (örn: Log4j, Struts2, DVWA) şeklinde ayağa kaldırılacak.
4. **Saldırgan Makine (Attacker & AI Host): Kali Linux**. Bu makine "Köprü" görevi görecek. Üzerinde hem manuel sızma araçları hem de bulut tabanlı zekayı kullanan **AI Ajanı (MCP)** çalışacak. Yapay zekanın kontrolden çıkmasını veya fiziksel ev ağına saldırmasını önlemek amacıyla, Python (Middleware) ve iptables (Hard Kill Switch) tabanlı **Güvenlik Kilitleri (Guardrails)** uygulanacak.
5. **Gözetleme Kulesi ve Otonom Savunma (SIEM):** Laboratuvara entegre edilen üçüncü sanal makine olarak **Wazuh Manager** kullanılacak. Bu sistem sadece logları merkezi olarak toplamakla kalmayacak; aynı zamanda saldırı anında kurban makineye müdahale emri vererek saldırganı otomatik olarak engelleyen **Active Response** (Otonom Savunma) mekanizmasını yürütecek.

6. **Hardening ve Otomasyon (DevSecOps):** Bulunan zafiyetler tespit edildikten sonra öncelikle manuel müdahele tecrübe edilecek sonrasında ise manuel yamalama yerine otomatize edilmiş operasyonlarla kapatılacak ve yapay zeka bir "Kalite Kontrol" (QA) asistanı gibi(yama önerisi istenecek) kullanılarak sistemin güvenli hale gelip gelmediği doğrulanacak.