**Velociraptor Nedir?**

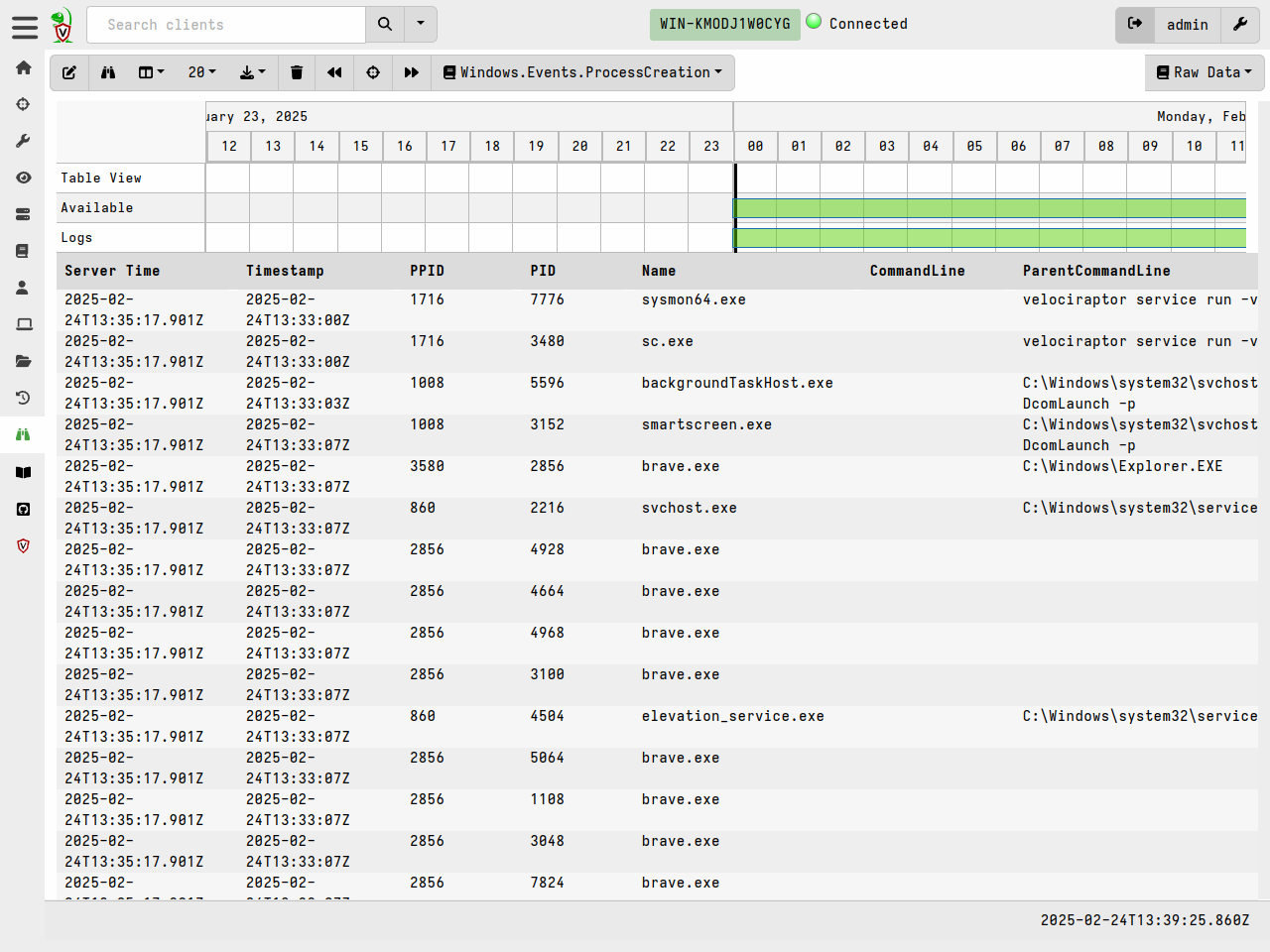
Velociraptor, siber güvenlik uzmanlarının bilgisayar sistemlerinde tehditleri araştırmasını (threat hunting) ve adli inceleme (digital forensics) yapmasını sağlayan açık kaynaklı bir araçtır.

Velociraptor, yüzlerce veya binlerce bilgisayardan veri toplayabilen, uzaktan bilgi alabilen ve şüpheli olayları tespit etmeye yarayan bir "dedektif programı"dır.

**Ne İşe Yarar?**

Velociraptor ile şunları yapabiliriz:

* Bilgisayarda şüpheli dosya, işlem veya bağlantı var mı kontrol etmek
* Kullanıcıların ne zaman giriş yaptığına bakmak
* Sistem günlüklerini (loglarını) incelemek
* Virüs bulaşmış bilgisayarı uzaktan tespit etmek
* Çok sayıda bilgisayarı aynı anda taramak
* Belirli komutları uzaktan çalıştırmak



Threat Hunting işlemi tamamlandıktan sonra, toplu veri indirme seçenekleri sunuluyor.

**Sunucu Kurulumu (Linux Örneği)**

Dosyayı çalıştır:

***chmod +x velociraptor-v0.7.1-linux-amd64***

***./velociraptor-v0.7.1-linux-amd64 config generate > server.config.yaml***

Sunucuyu başlat:

***./velociraptor-v0.7.1-linux-amd64 -config server.config.yaml frontend***

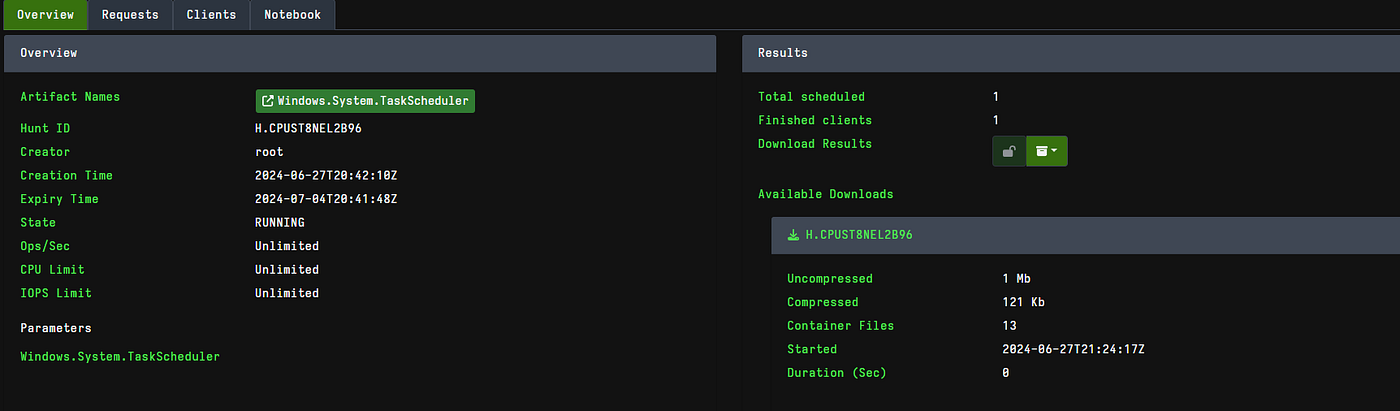
Web arayüzüne giriş:

Tarayıcıda şunu aç:

**cpp**

***https://<sunucu-ip-adresi>:8889***

Varsayılan kullanıcı adı ve şifre genellikle ilk kurulumda belirlenir.



GUI üzerinde bağlı istemcilerin listesi, aktif bağlantılar ve işlem detayları yer alıyor.

**İstemci Kurulumu (Windows)**

İstemci bilgisayarda şu adımlar izlenir:

İndirdiğin .exe dosyasını çalıştır.

Aşağıdaki komutla istemci yapılandırmasını al:

***velociraptor-v0.7.1-windows-amd64.exe config client --config server.config.yaml > client.config.yaml***

Ardından istemciyi başlat:

***velociraptor-v0.7.1-windows-amd64.exe -config client.config.yaml client***

İstemci başlatıldığında sunucuya bağlanır ve izlenmeye hazır hale gelir.

**Artı ve Eksi Yönleri**

**Artıları**

* Açık kaynak ve ücretsiz
* Çok hızlı veri toplama
* Güçlü filtreleme ve sorgu sistemi
* Gerçek zamanlı izleme yeteneği
* Windows, Linux ve Mac desteği

**Eksileri**

* İlk öğrenme eğrisi biraz yüksek (özellikle query kısmı)
* Sunucu ve istemci kurulumu karışık olabilir
* İngilizce arayüz

Velociraptor, hem bireysel bilgisayarlarda hem de büyük kurumsal ortamlarda adli inceleme, tehdit avcılığı ve sistem denetimi için kullanılabilen modern ve güçlü bir araçtır. Eğitim ortamlarında, öğrencilere uzaktan analiz ve veri toplama mantığını öğretmek için idealdir.