Uygulamalı Beyaz Şapkalı Hacker Eğitimi

Zafiyet Keşfi

Konular

- Zafiyet Nedir?
- Zafiyetin Kaynağı Nedir?
- Zafiyet Yönetim Döngüsü
- Otomatize Zafiyet Tarayıcıları
- Zafiyet Veritabanları
- Sık Kullanılan Araçlar
- Uygulamalar

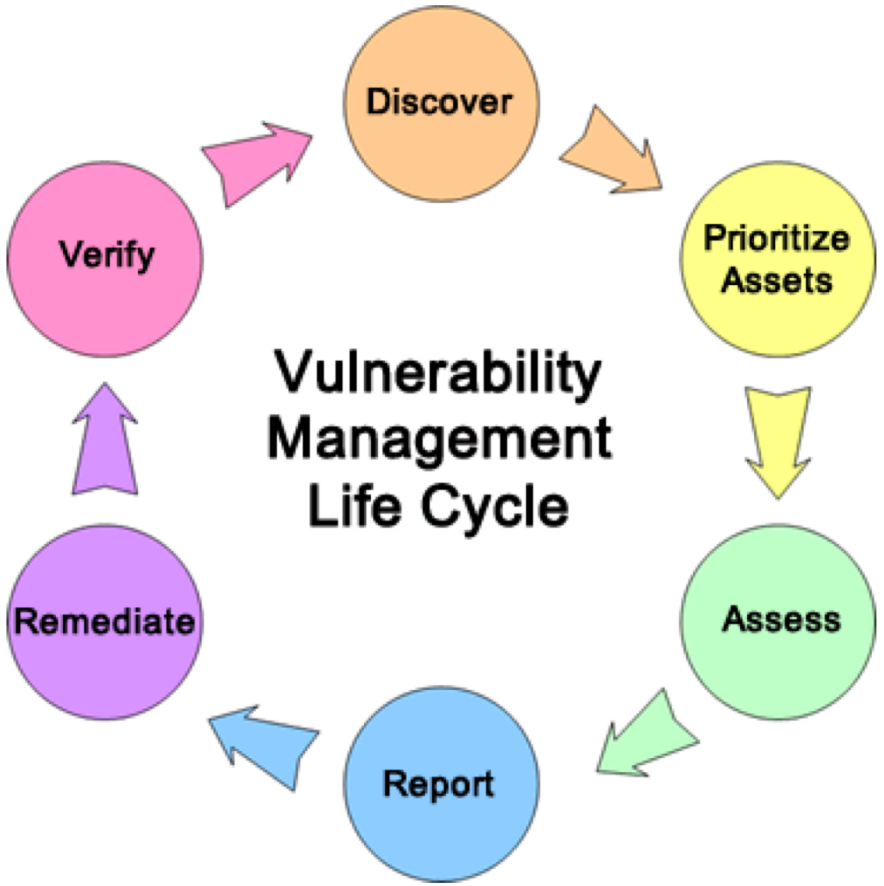
Zafiyet Nedir?

- Herhangi bir uygulamada, servis veya protokolde, daha önce yapılan araştırmalarda tespit edilmiş veya yeni keşfedilen ve siber saldırganlar için bir atak türüne izin veren, sistemin akışını etkileyebilecek zayıflıklardır.
- [Senaryo]

Zafiyetin Kaynağı Nedir?

- Eski sürüm / güncellenmemiş uygulama ve servisler
- Yama eksiklikleri
- Hatalı konfigürasyonlar
- Güvenli yazılım geliştirme süreç eksiklikleri
- Güvensiz ağ mimarisi tasarımları
- Insider, bilinçsizlik

Zafiyet Yönetim Döngüsü



Zafiyet Tarayıcıları

- Netsparker
- Acunetix
- Burpsuite
- Appscan
- Webinspect
- W3af
- Arachni
- Nikto
- Sqlmap
- Nessus
- Nexpose
- OpenVAS
- Qualys
- Core Impact
- Vega
- Skipfish
- Commix
- nmap

Neden ihtiyaç duyarız?

- Riski tanı!
- Riski yönet!
- Olası siber saldırıların bir nebze de olsa önüne geç!
- Wannacry vakası!
- Geçmişte yaşanan siber olaylardan ders çıkar!

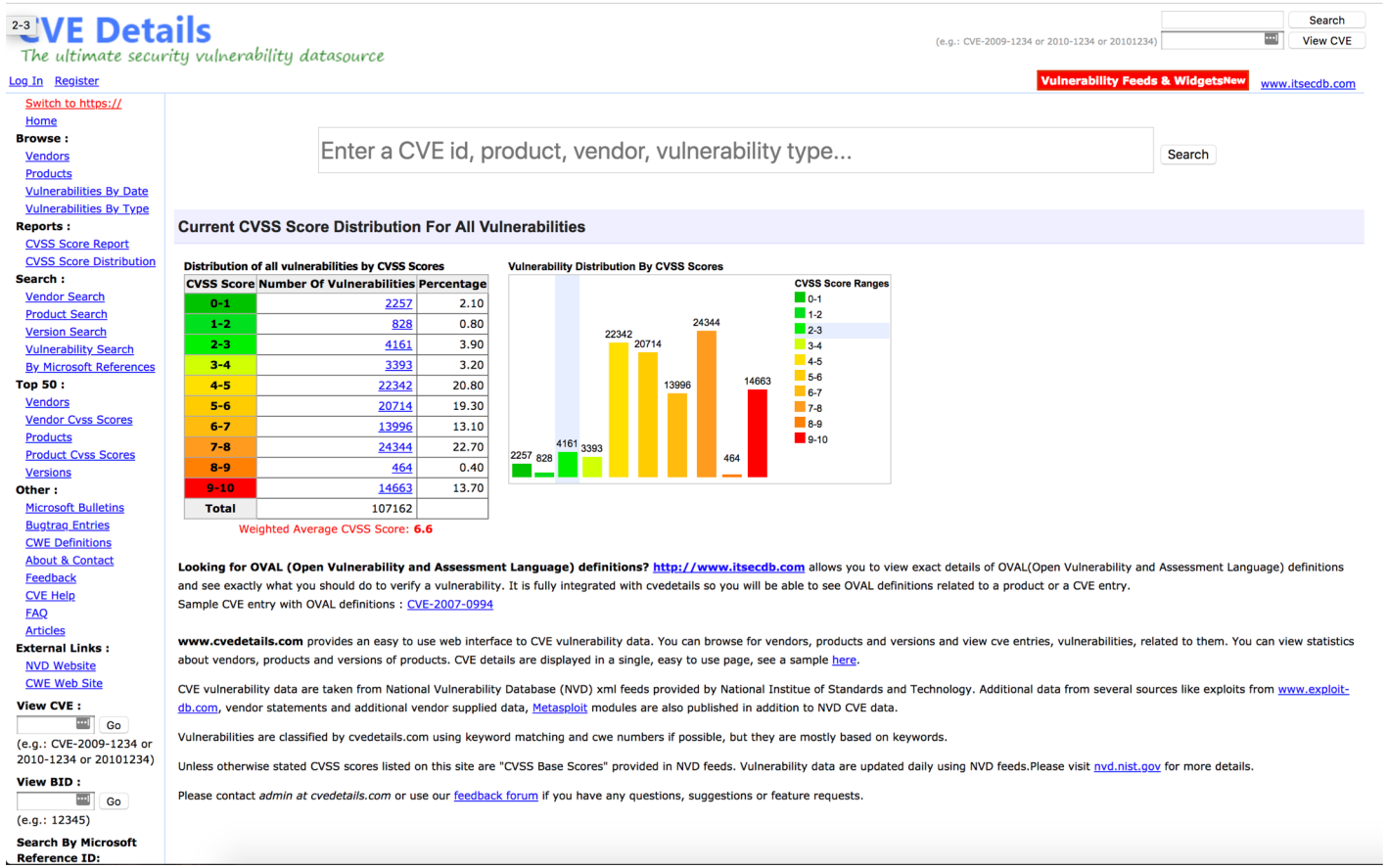
Anahtar Kelimeler

- POLICY: Gerçekleştirilecek taramalar için yapılan özel ayarlamalara verilen isimdir. Örneğin ağ taramalarında kullandığını POLICY ile web uygulamaları taraması için kullandığınız POLICY farklılık gösterir.
- PLUGIN: Güvenlik kontrolleri için geliştirilmiş olan küçük araçlar/scriptlerdir.
- SCAN: Tarama işlemi

Zafiyet Veritabanları

- Zafiyet veritabanları tespit edilmiş olan zafiyetlerin listelendiği veritabanlarıdır.

- https://nvd.nist.gov/
- https://www.cvedetails.com/

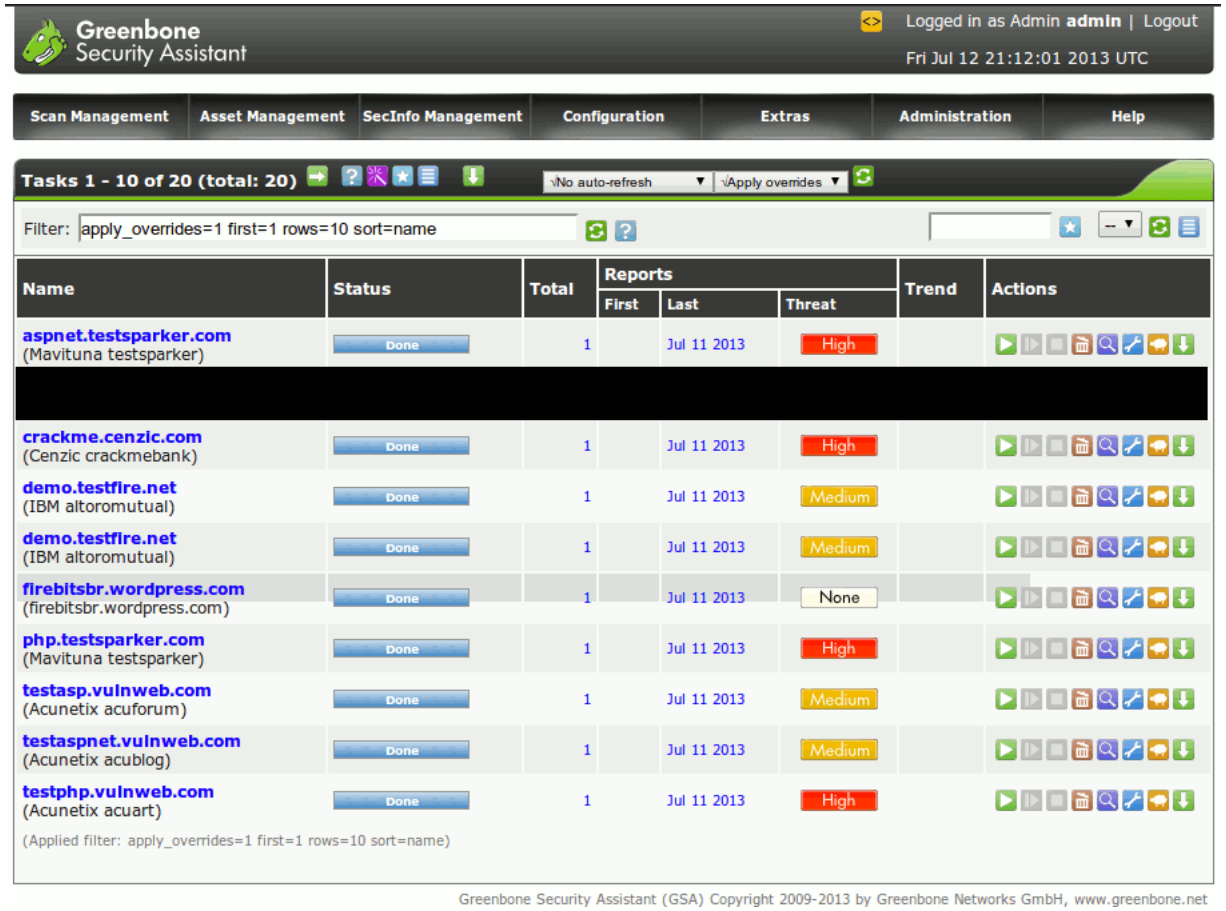


Güvenlik Tarayıcıları

- All In One mantığı
- Network üzerindeki zafiyetleri bulmakta daha iyiler
- Daha çok sunucu/istemci tabanlı zafiyetlerin kontrollerinde kullanılıyorlar
- Uyumluluk, konfigürasyon, zafiyet testleri
- False positive durumlarla karşılaşılıyor
- Test süresini ciddi oranda kısaltıyor

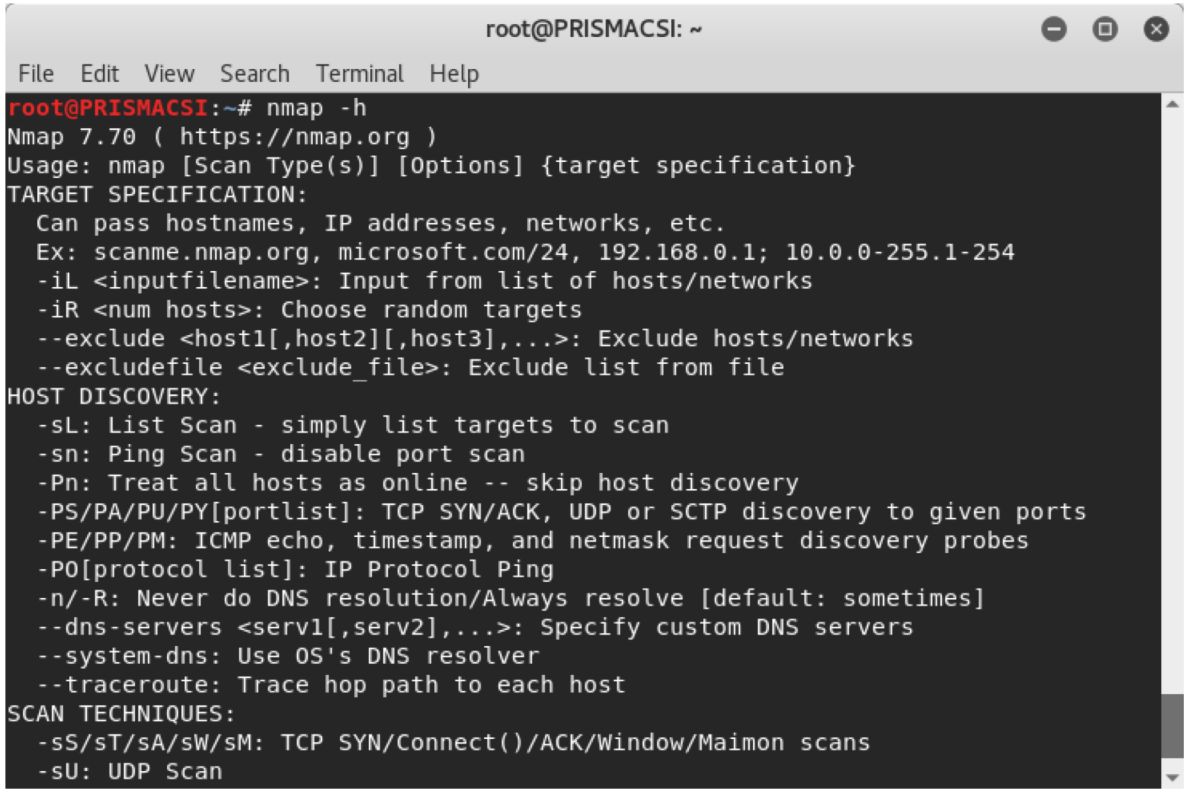
OpenVAS Security Scanner - DEMO

- Açık kaynak zafiyet tarama aracıdır.
- İçinde gelişmiş özellikler barındırır.
- Nessus alternatifi olarak kullanılabilir.



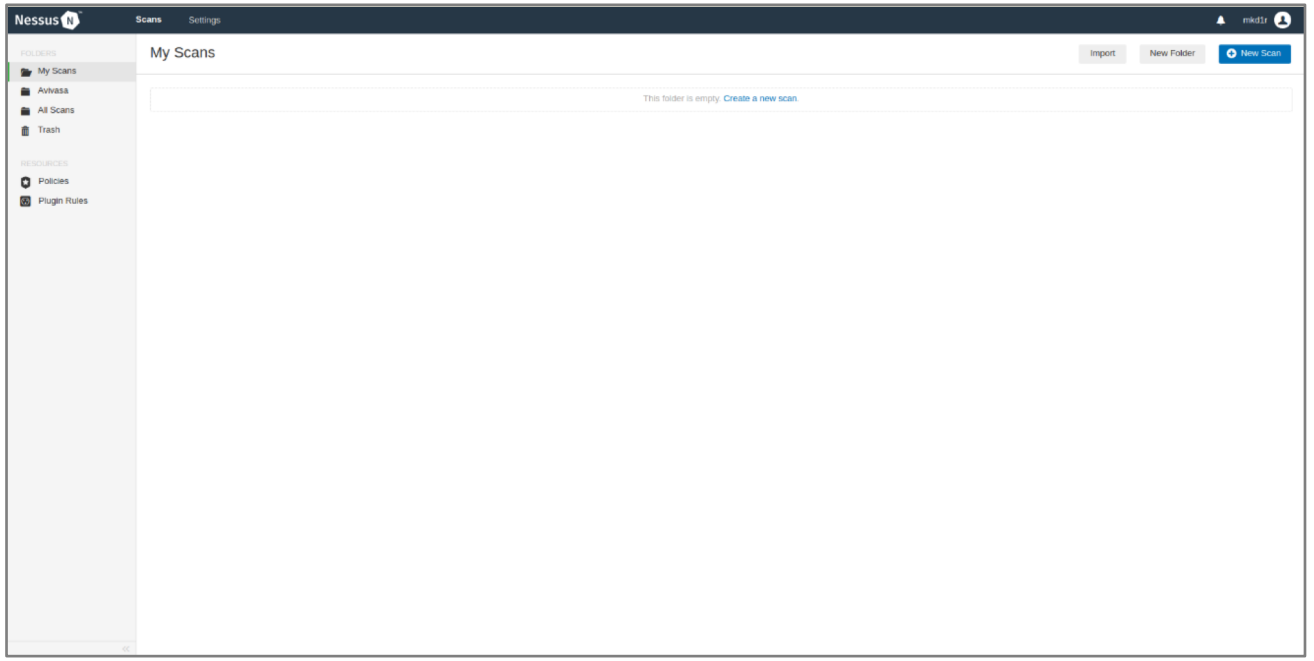
Nmap NSE - DEMO

- Nmap Scripting Engine ile zafiyet taraması yapmak mümkündür.
- Açık kaynak yazılım. Siz de katkı verebilirsiniz ve üstüne modüller geliştirebilirsiniz.
- Hızlı tarama imkanı veriyor.
- Genelde tüm testlere nmap zafiyet taramaları ile başlanır.



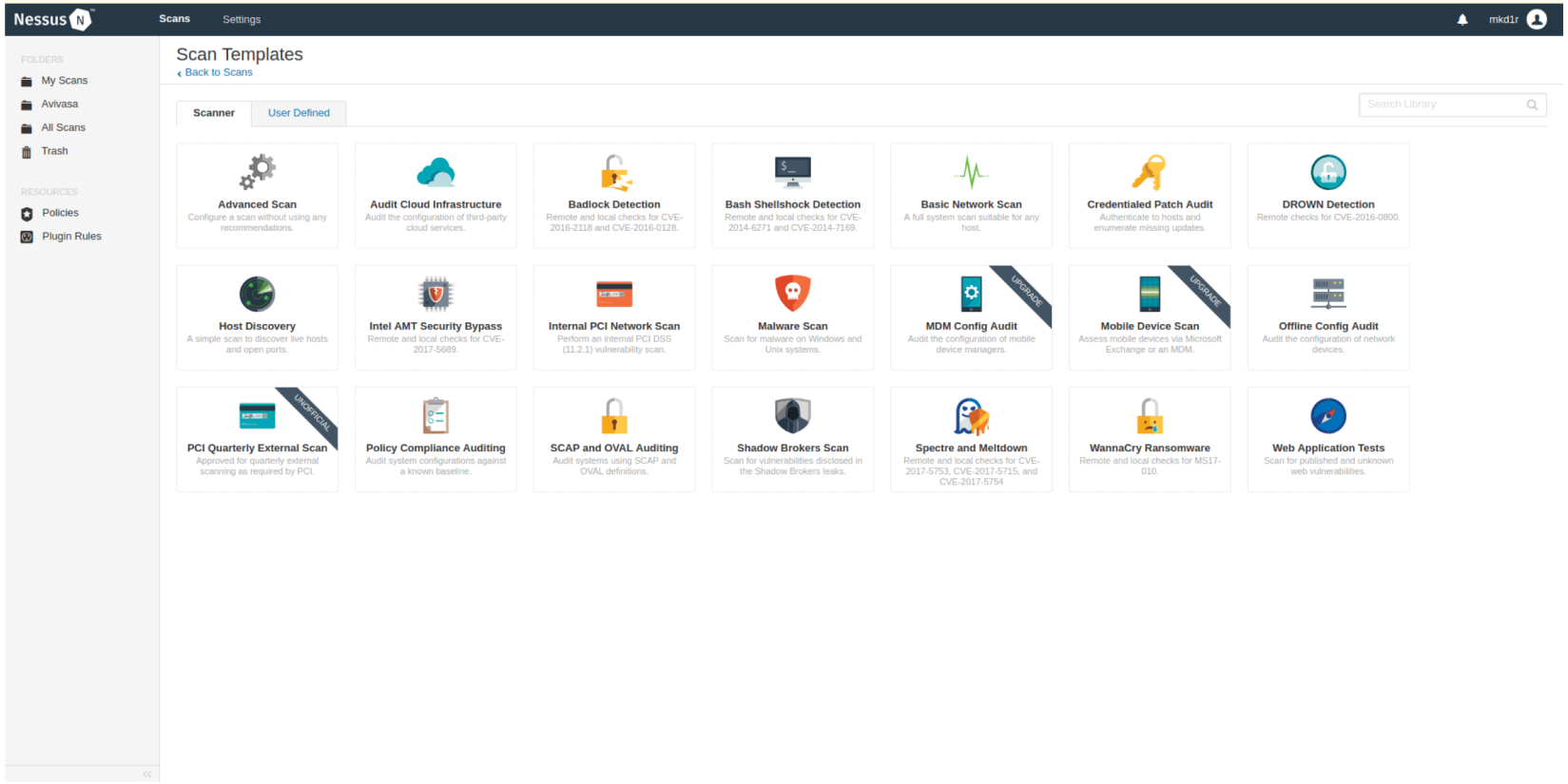
Nessus - Uygulama

- En sık kullanılan zafiyet tarama aracıdır.
- Penetration test vs zafiyet taraması konusuna geri dönüş!
- Lisanslı ve Free sürümleri mevcuttur.
- Free sürüm ile de birçok güvenlik kontrolünü gerçekleştirebilirsiniz.
- Web, Network, SCADA, Uyumluluk taramaları gibi seçenekler mevcuttur.
- Daha çok network taramalarında kullanılır.



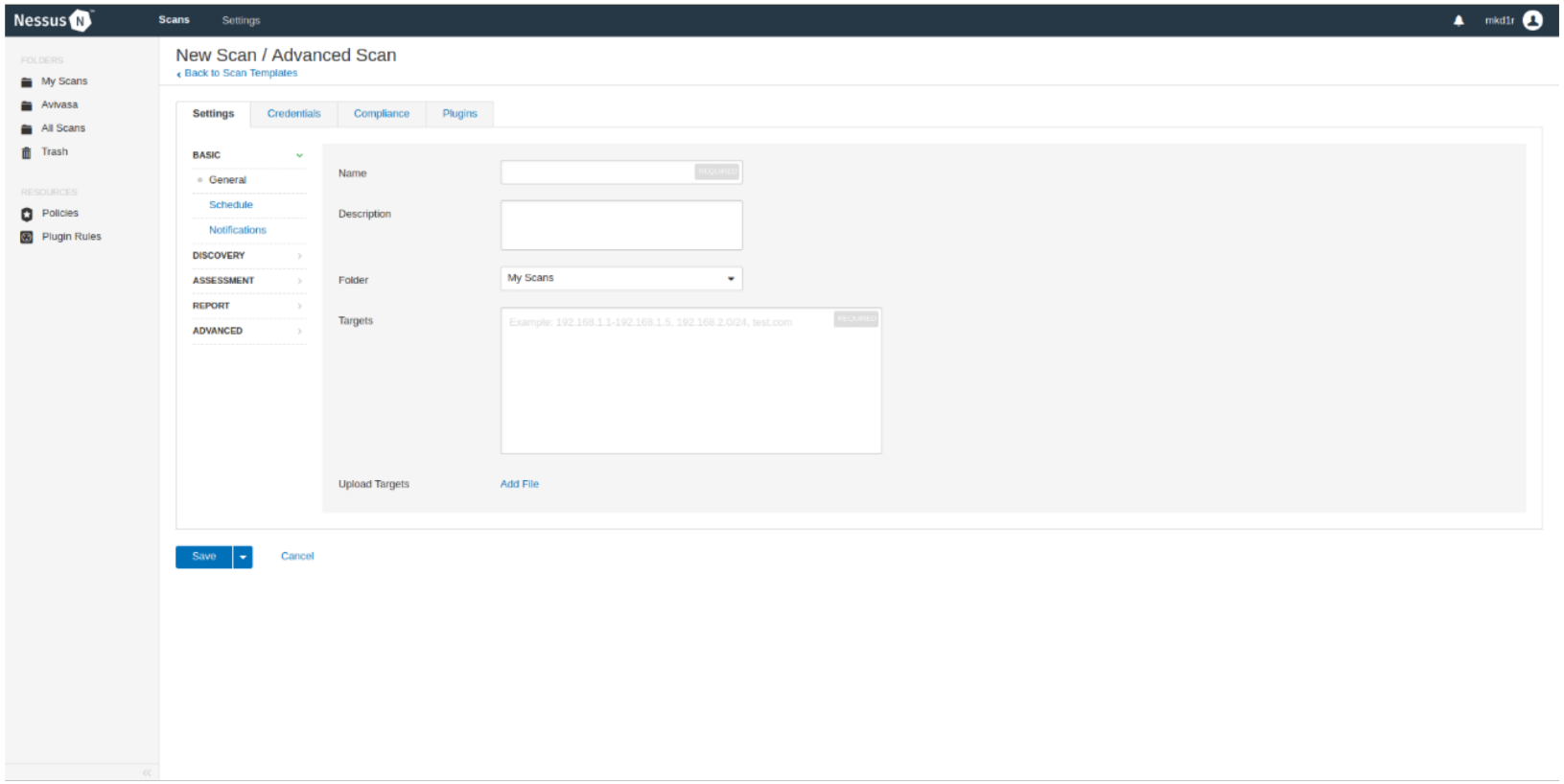
Nessus - Uygulama

- Yeni Tarama Başlatma
  - Policy
  - Gelişmiş Tarama
  - Düzenlenebilir
  - Taramayı kendinize göre özelleştirebilirsiniz ve gelişmiş ayarlar yapabilirsiniz.



Nessus - Uygulama

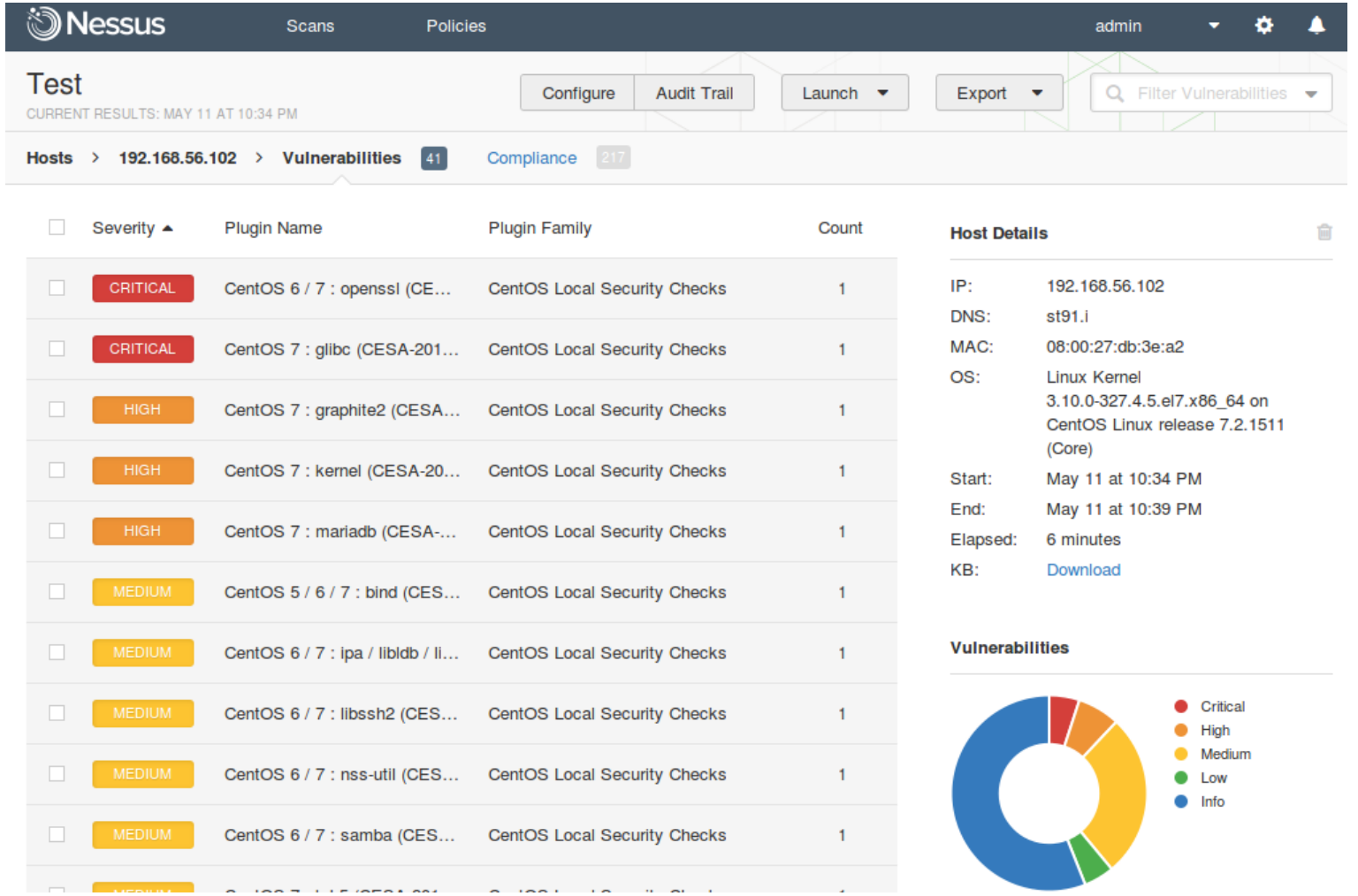
- Yeni Tarama
  - Hedef Sistemler
  - Pluginler
  - Zamanlama ayarları
  - Kaba kuvvet saldırıları
  - Gelişmiş Ayarlar



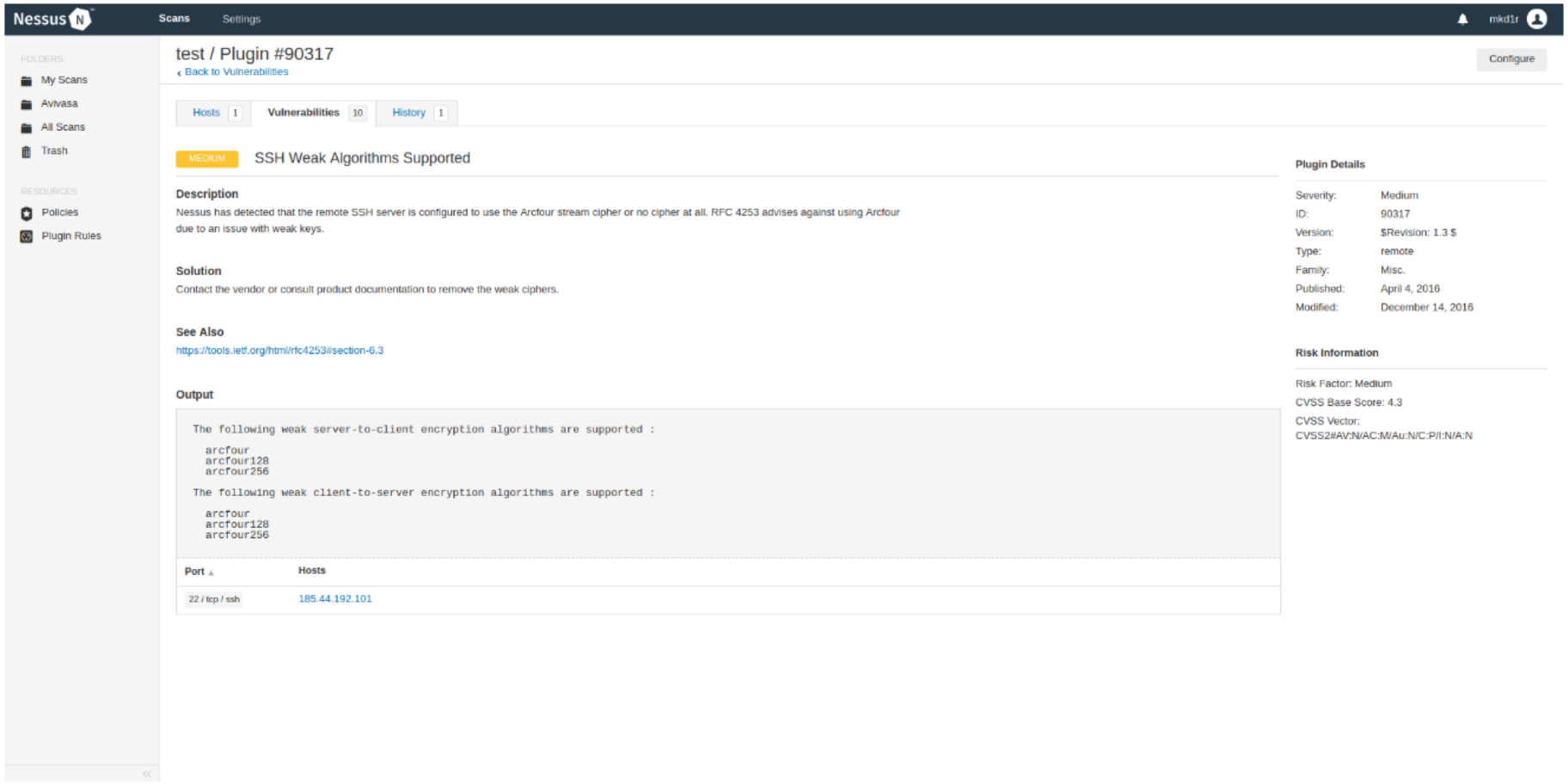
Nessus - Uygulama

- Tarama sonuçları birçok farklı formatta sunuluyor. Bu çıktılar ile büyük bir ağın dahi kolayca analizi yapılabilir.
  - Detaylı analiz
  - Kritiklik Seviyeleri

Nessus - Uygulama

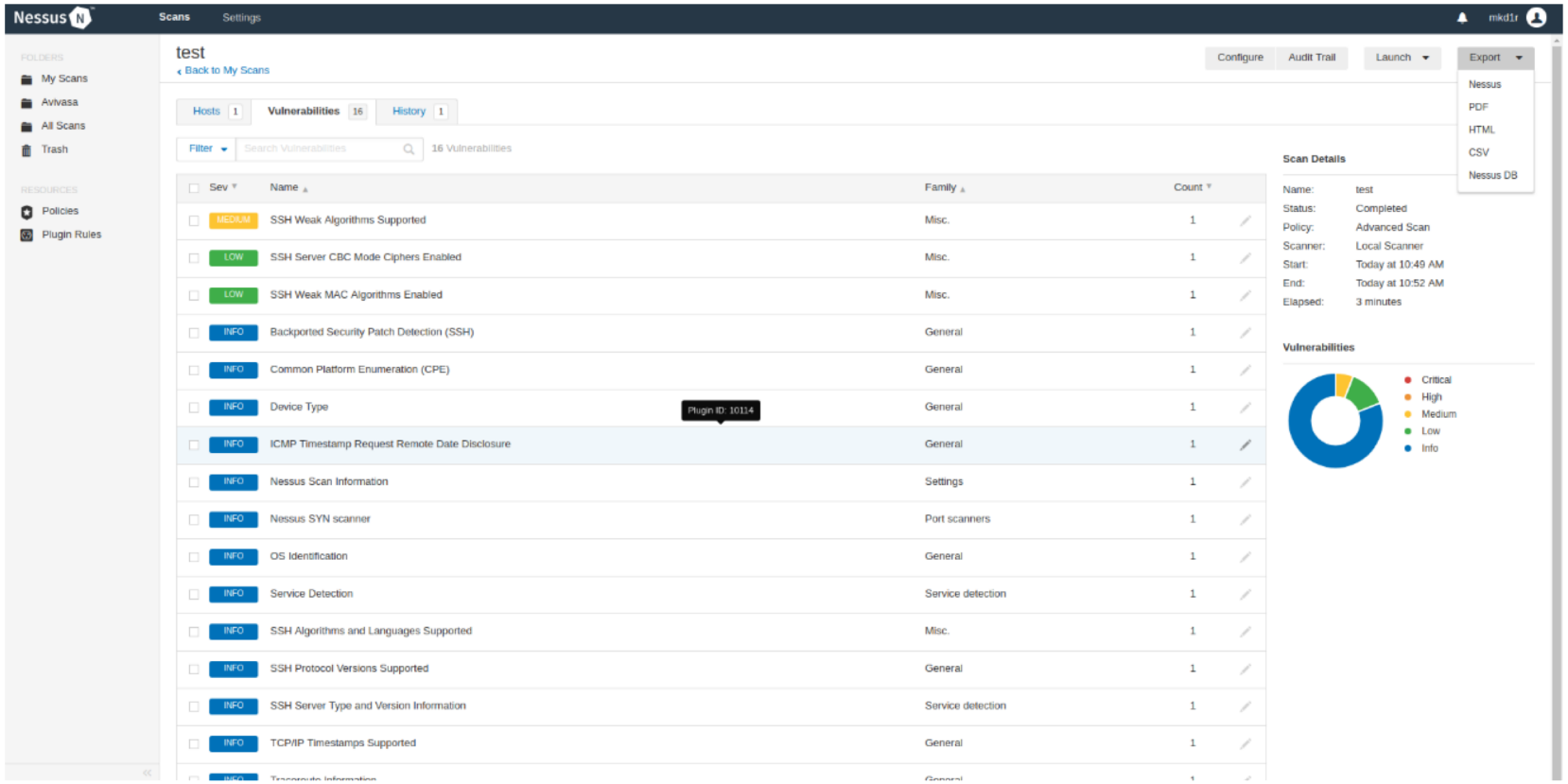


Nessus - Uygulama



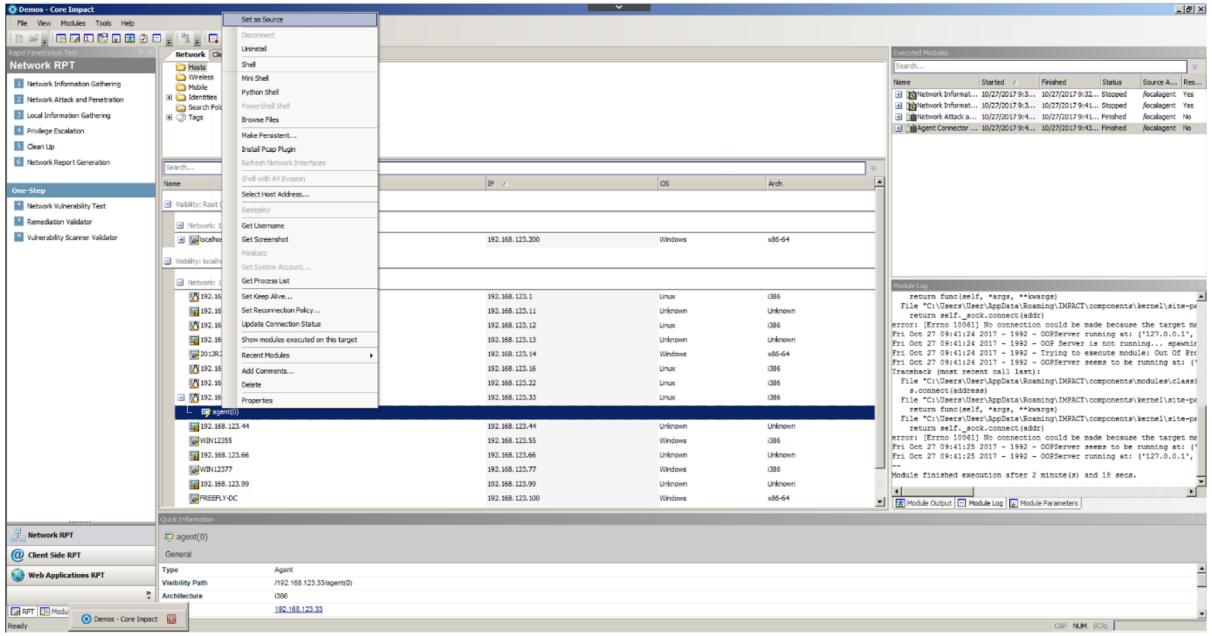
Nessus - Uygulama

- Tarama raporu aşağıdaki formatlarda sunulmaktadır ve bu formattaki çıktılar ile birlikte diğer penetration test araçları ile entegre çalışılabilmektedir.
  - Formatlar
    - XML
    - HTML
    - Nessus



Core Impact - Tanıtım

- Security Scanner
- İçerisinde ileri seviye birçok güvenlik kontrolü mevcut ve kendine has araçları da barındırıyor.
- Özel exploitler mevcuttur.
- Özel Zeroday ekibi vardır.
- Lisans bedeli ☺

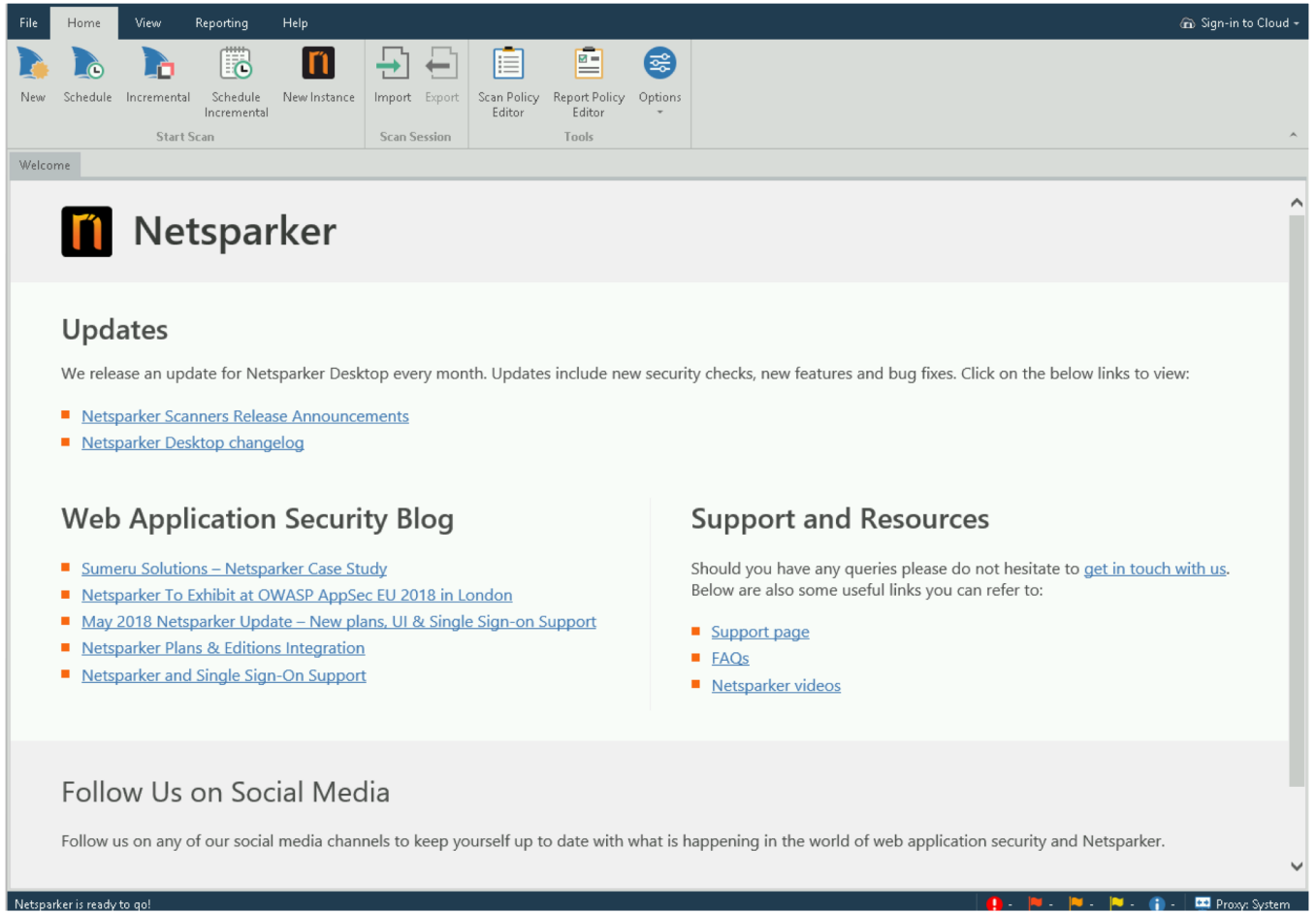


Web Güvenlik Tarayıcıları

- Web uygulamaları ve servislerinin güvenlik taramaları için kullanılıyor
- Manuel testlere de imkan sağlayanları mevcut
- Netsparker Dünya genelinde kabul edilmiş en başarılı zafiyet tarayıcısı
- Burp suite en kritik araç!

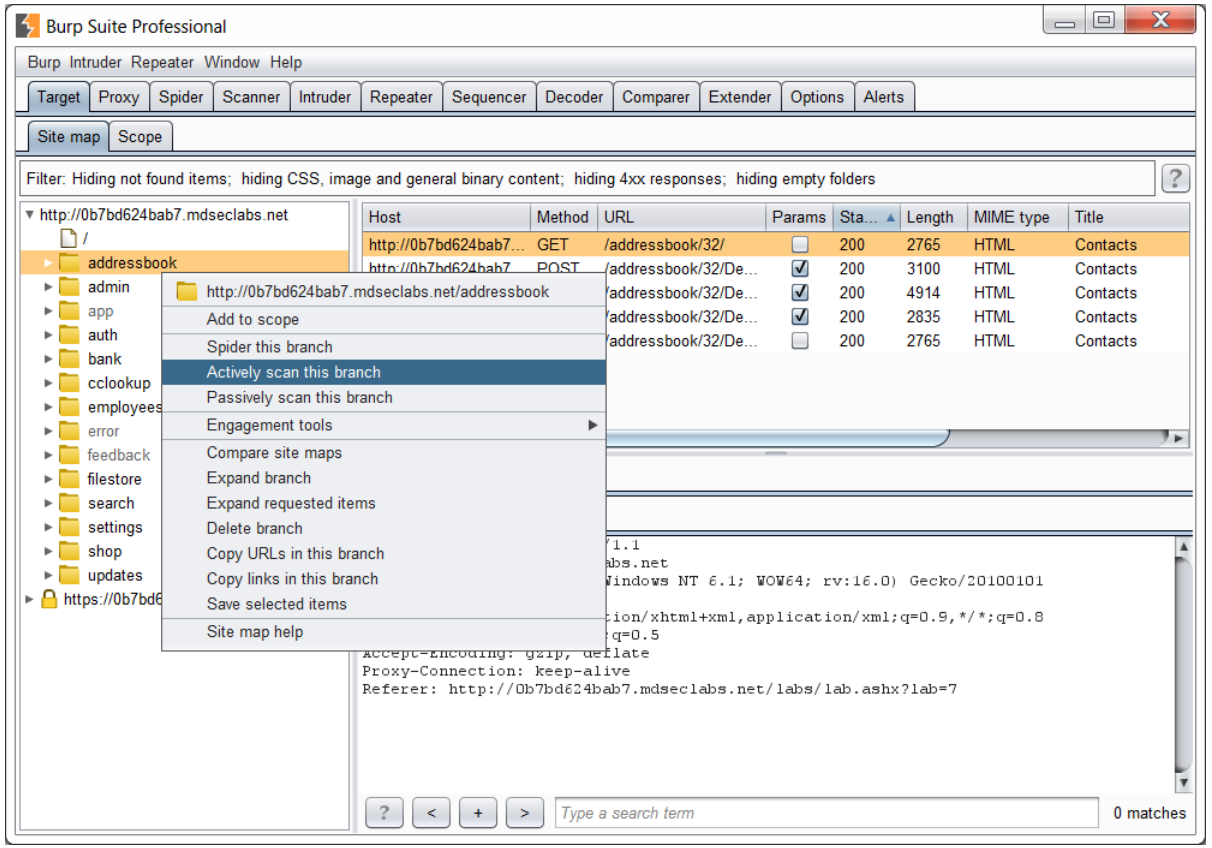
Netsparker - Uygulama

- Web uygulama güvenlik tarama aracı
- Lisanslı ve Free sürümleri mevcut
- Web teknolojileri özelinde geliştirilmiş bir yazılım.
- Netsparker Cloud ile birlikte daha gelişmiş ve entegre çözüm



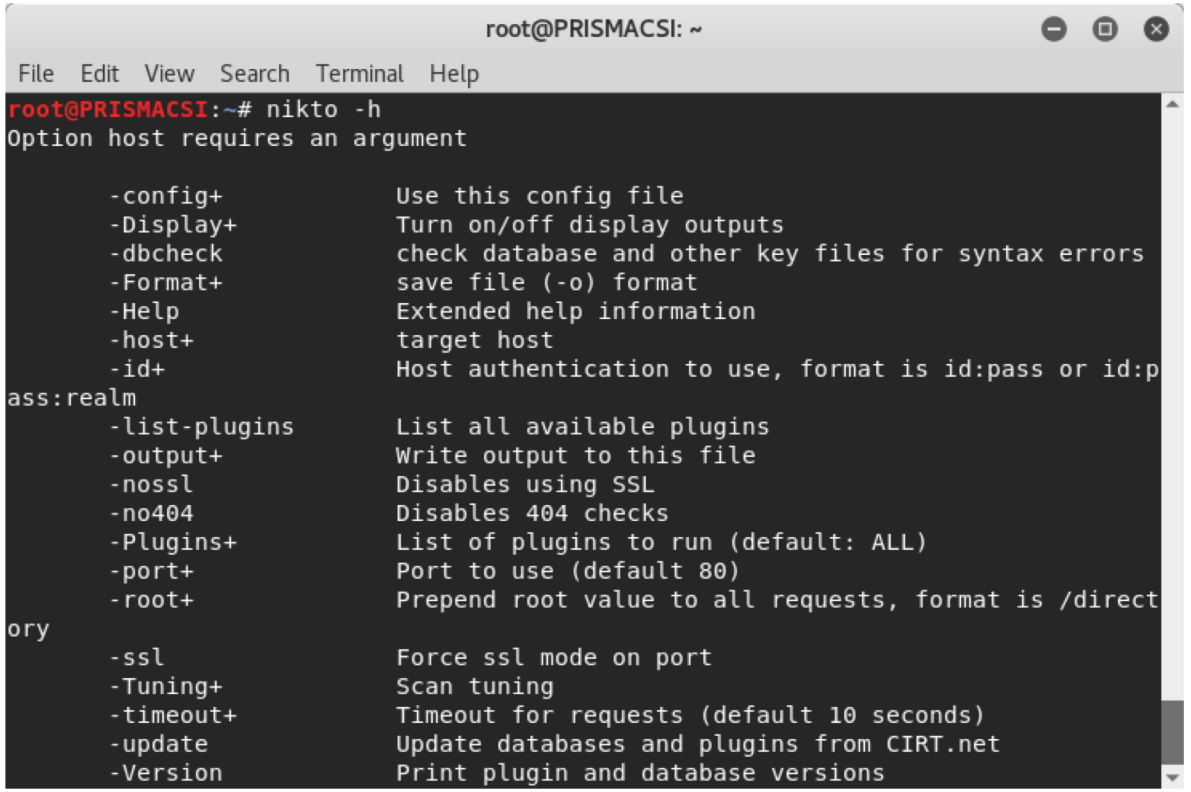
Burpsuite - Uygulama

- Web uygulama Proxy aracı ve Güvenlik Tarayıcısı
- Lisanslı ve Free sürümü var
- Web teknolojileri özelinde
- En kullanışlı araç
- Hackerların, Pentesterların eli kolu



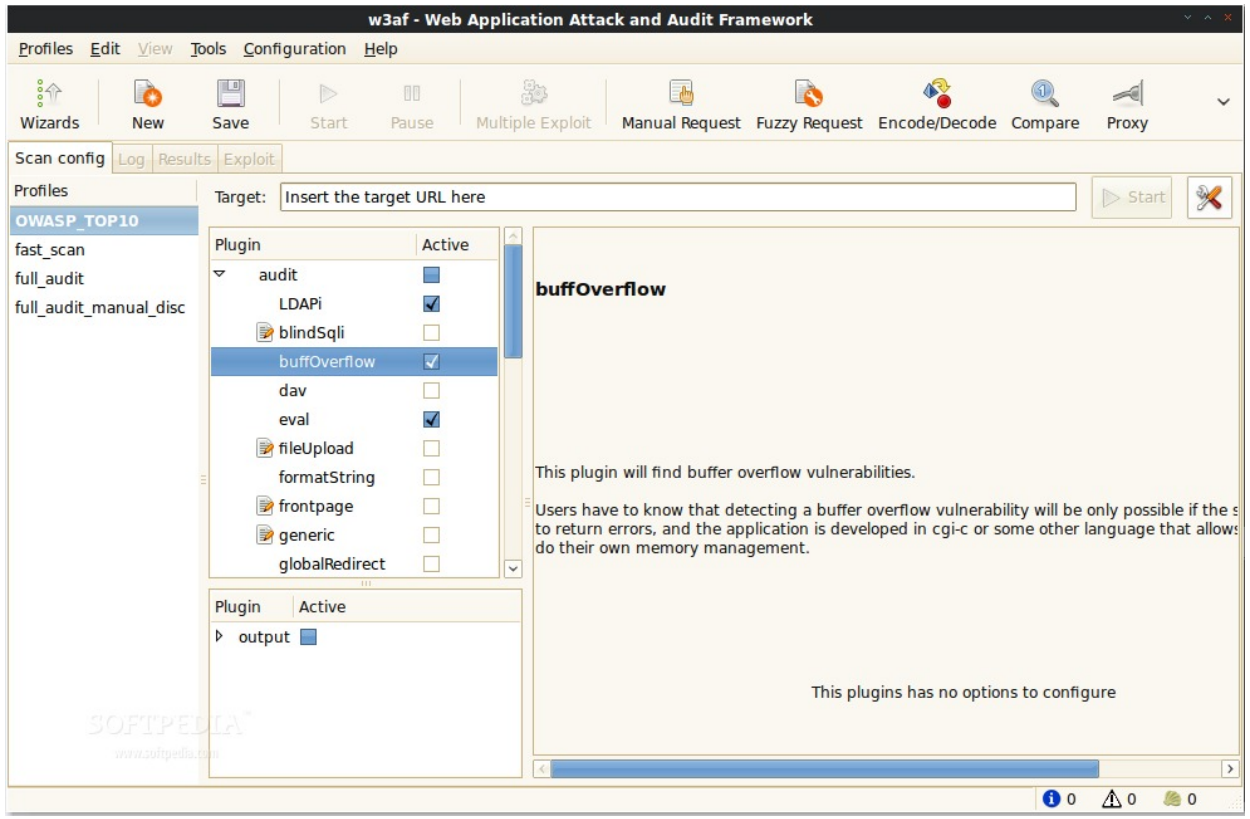
Nikto Security Scanner - Uygulama

- Web uygulama ve sunucu güvenlik tarayıcısıdır.
- Sık kullanılan pratik bir uygulamadır.
- Komut satırı üzerinden kullanılır.



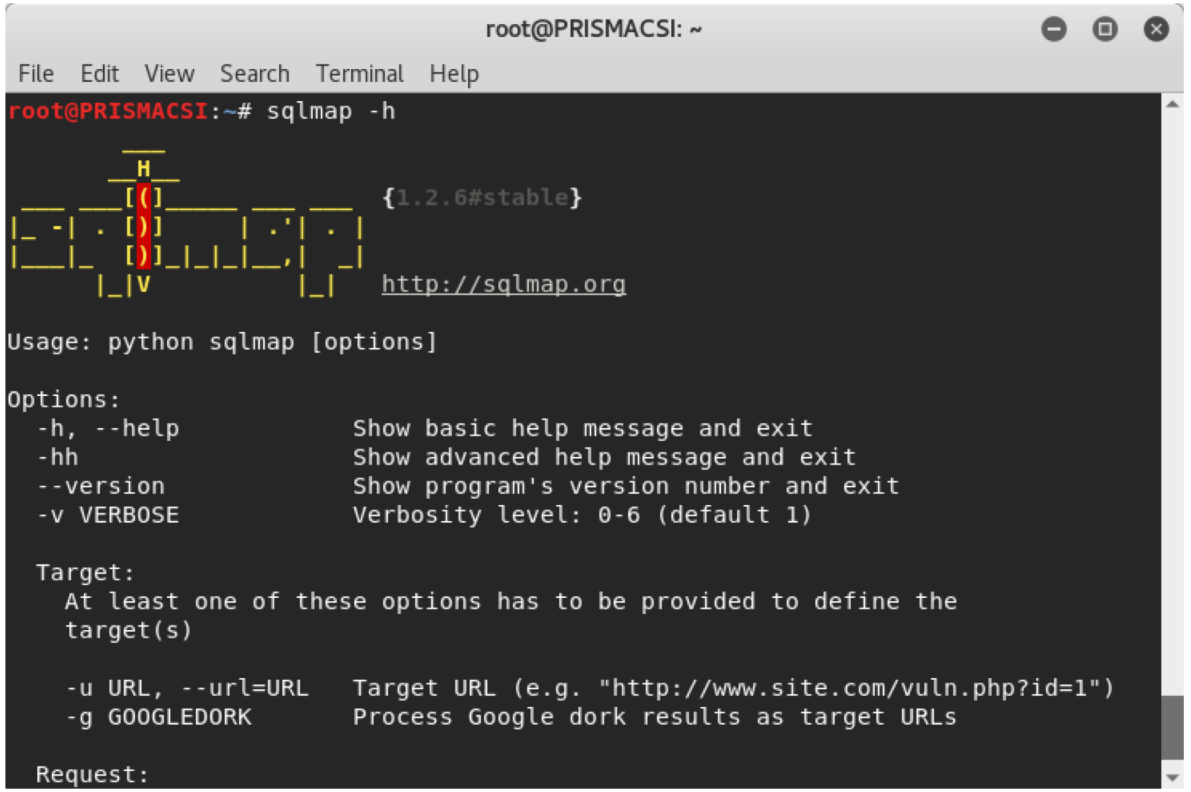
W3af Web Scanner - Uygulama

- Web uygulama güvenlik tarayıcısıdır.
- OWASP tarafından geliştiriliyor.
- İçinde politikalar mevcut ve özelleştirilmiş taramalar yapılabiliyor.
- Sık kullanılmasa da oldukça kullanışlıdır.



Sqlmap – SQL Injection Scanner – Uygulama

- SQL Injection saldırıları için özel olarak geliştirilmiştir.
- Python programlama dili ile geliştirilmekte
- Açık kaynak
- Gelişmiş parametrelere ve atak methodlarına sahip



Zafiyetler sadece uzaktan mı kontrol edilir?

- Bir tarama sadece uzaktan web uygulamasına yönelik veya bir sunucuya yönelik gerçekleştirilmek zorunda değil.
- Aynı zamanda bir sunucunun içerisine giriş yaparak işletim sistemi özelinde de tarama gerçekleştirilebilir. (RDP, SSH login –> içeride tarama)
- Uyumluluk veya konfigürasyon kontrolleri gerçekleştirilebilir
- Statik kod analizi gerçekleştirilebilir

Sonuç olarak:

- Elimizde en başta topladığımız bir çok istihbarat verisi var.
- Artık karşımızda var olan ve ayakta olan sistemleri tanıyoruz.
- Bu sistemlerde açık portları keşfettik ve bu portlar üzerinde çalışan yazılımları biliyoruz.
- Bu yazılımlar üstünde çalışan uygulamalarda var olan veya servisler üzerinde keşfettiğimiz açıklıkları da kenara not ettik.
- Şimdi sırada bu zafiyetleri nasıl kullanacağımızı kavramakta!

UYGULAMALAR

SORULAR?