

Bilgi Sistemleri ve Güvenliği Dersi Bireysel Rapor

190542007

Bedirhan TUNCER

Giriş

Bu rapor, Bilgi Sistemleri ve Güvenliği dersinin işleyişi gereği 01.08.2022 – 26.08.2022 tarihleri arasında grup halinde gerçekleştirdiğimiz tarama araçları kullanımı ve sızma testlerinde bireysel olarak neler yapıp, neler yapamadığımı içerendetaylı bir rapordur.

Yaptığımız çalışmalar sonucunda bilgi farkındalığı ve bilgi güvenliğini önemini sonuç olarak elde etmiş oldum. Yazılım Mühendisi olarak tarama araçları ve Kali işletim sistemine olan yabancılığımı giderdim. Bir web sayfasının güvenliğini temel seviyede kontrol edecek ve önlem alacak bilgim var.

Özet

Grup dağılımları sonucu bulunduğum 4 numaralı grup içerisinde iletişimi sağlayan, grup üyeleri arasında köprü niteliğinde bir rolde bulundum. Grup sayımızın 17 kişi olması sebebiyle etkin bir çalışma yapabilmemiz için dörtlü grupları ayrılmaya karar kıldık. Grup dağılımı ve görev dağılımını yaptıktan sonra içerisinde bulunduğum ekip ise Nessus tarama aracını tanıttı.

*Bu grup içerisinde Nessus kurulumu, tarama işlemi ve sunum noktasında yardımcı oldum. Bunun yanı sıra sunucu bendim.

Tüm tarama araçları ile Muş Ticaret ve Sanayi Odası'nın taraması yapıldıktan sonra raporlama ve Nessus tarama aracından elde ettiğimiz sonuçlarının sunumunu yaptım.

Yaptığım Tarama ve Araştırmalar

- 1. Nessus Kurulumu
- 2. Nessus ile Güvenlik Açıklarının tespiti
- 3. Basic Network Scan

1. Nessus Kurulumu

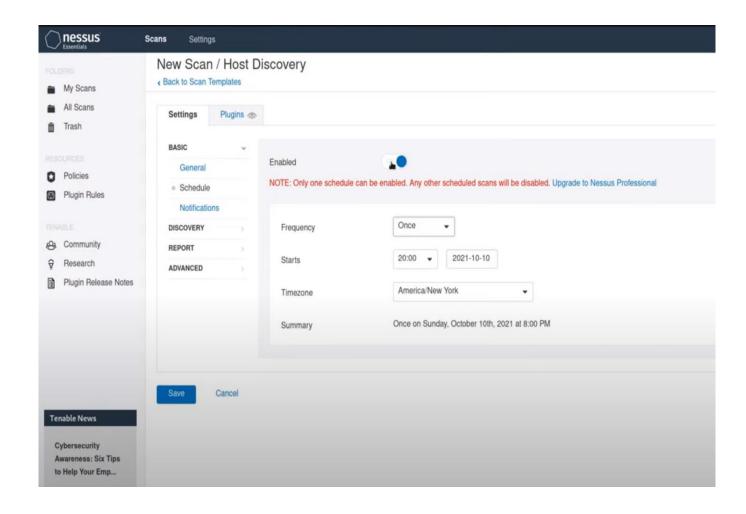
Nessus'u bir sunucuya kurmak, eğitimsiz bir yönetici için oldukça zordur. Her şeyden önce, Unix için önceden yüklenmiş bir sürüme ihtiyaç vardır. Ayrıca, bir bağlantı noktası tarayıcısı için kabul edilen bir standart **NMAP**, iyi bir şifre test cihazı Hydra ve son olarak iyi bir CGI tarayıcısı **Nikto** gibi bazı ek uygulamaların yüklenmesi önerilir. Bu programların yüklenmesi gerekmese de, Nessus'un performansını büyük ölçüde artıracaklar. UNIX sistemleri için sınıflarında en iyi yardımcı programlar olarak kabul edildikleri için önerilir.

Kali'ye girdikten sonra terminal kısmına:

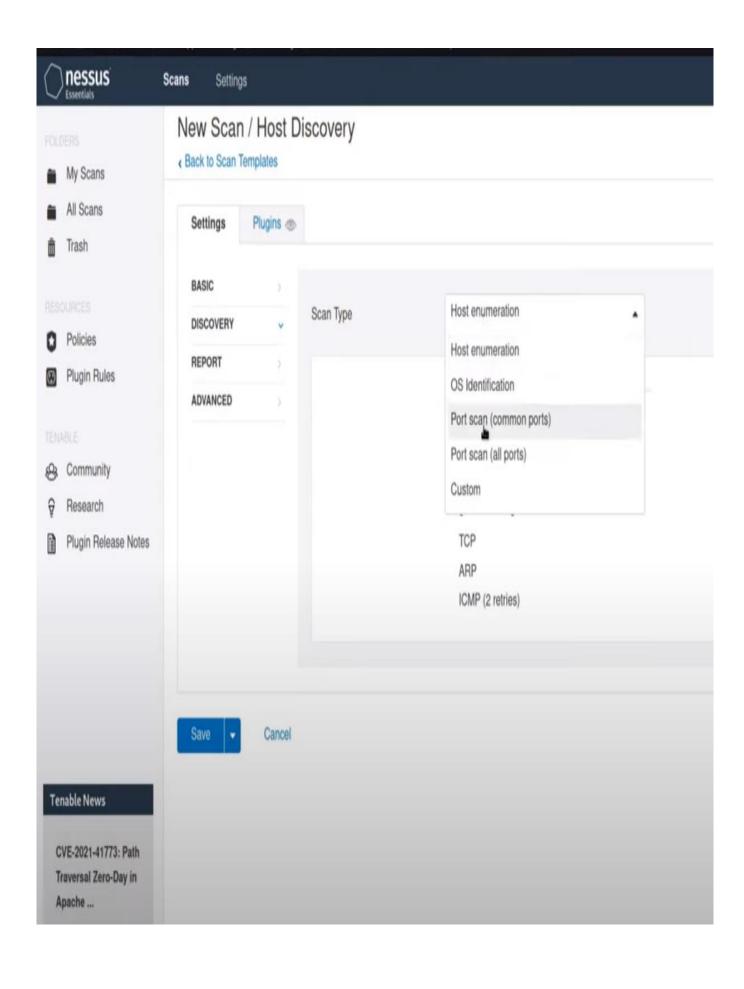
Lynx -source http://install.nessus.org | sh

2. Nessus ile Güvenlik Açıklarının tespiti

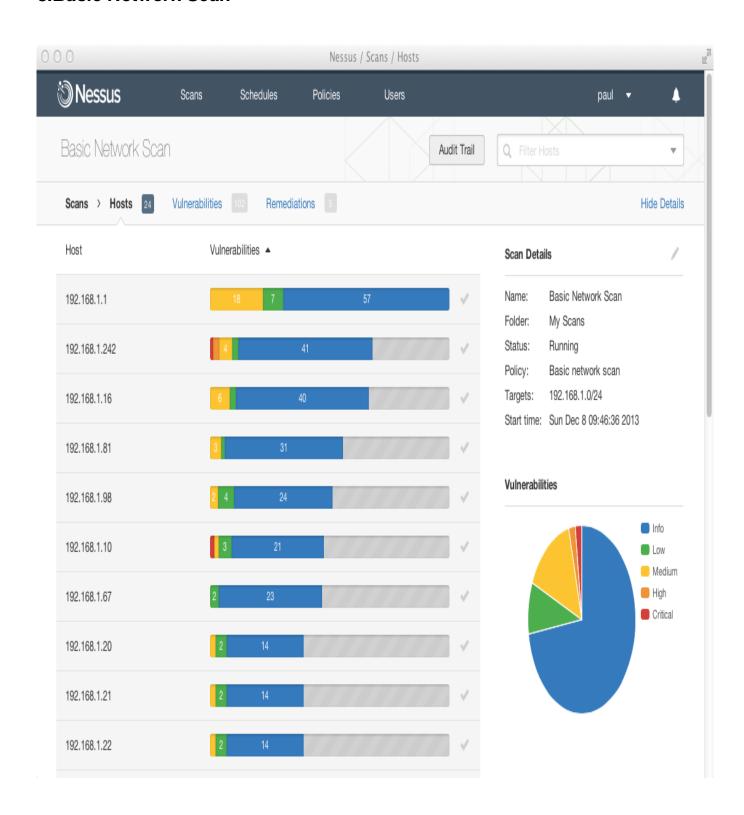
- Hassas verilere erişmesine veya bunları kontrol etmesine veren güvenlik açıklarının tespiti,
- Yanlış yapılandırma sorunlarının önceden bilinmesi,
- Varsayılan şifre ya da kolay şifre kullanımı gibi sistem üzerindeki sorunların tespiti,
- ▶ DDoS (Hizmet dışı bırakma) saldırılarına izin veren TCP/IP sorunlarının çözümü,
- Yüksek hızda varlık keşfi,
- Yama ve yapılandırma denetlemesinin yapılması,
- Varlık profili çıkarma,
- Hassas veri keşfi,
- Yama yönetimi entegrasyonu,
- Çoklu tarayıcı yönetimi ve zafiyet analizi.



Schedula sekmesinde hangi tarih ve saat aralığında scan'ı başlatacağımızı seçebiliyoruz. Aynı anda birden fazlascan ekleyebilmek için profesyonel paketi yüklememiz gerekiyor



3.Basic Network Scan



Sonuç

Yaz dönemi itibariyle Bilgi Sistemleri ve Güvenliği dersinden elde ettiğim çıkarımlar:

- Bilgi Güvenliği Farkındalığı noktasında yetkin bir noktaya geldiğimi düşünüyorum.
- Dersin üçgenin bir köşesinde bulunan kriptoloji kısmında hala derse başladığımız noktadayım.
- Penetrasyon testi kısmında ise yaptığımız laboratuvar uygulamaları, grup çalışmaları ve tarama araçlarının kullanımı ile oldukça verim aldım ve kendimi geliştirdim.
- Ekip ile çalışmanın zorlukları ve kolaylıkları kısmında gözlemleme yapabildim.
- Üyeler ve gruplar arası iletişim noktasında kendimi geliştirdiğimi düşünüyorum.
- Ders işleyişi gereği fazlasıyla sunum yaptığımızdan dolayı bu noktada tecrübelenmekten dolayı oldukça mutluyum.
- Tarama araçları ve kali işletim sisteminin herkesin ulaşabileceği şeyler olduğunu gördüm. Doğrusu yalnızca kapüşonlu gözleri kapalı kod yazan insanların uğraşı olduğu algımı yıktım diyebilirim.
- Raporlama noktasında başladığım noktaya nazaran yol kat ettiğimi düşünüyorum