Bilgi Sistemleri ve Güvenliği Dersi
Bireysel Rapor

175541038

Muhammet Can Görücü

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 içeren detaylı 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 etki sahibi olduğumu düşünüyorum.

Özet

Grup dağılımları sonucu bulunduğum 2 numaralı grup içerisinde iletişimi sağlayan, grup üyeleri arasında köprü niteliğinde bir rolde bulundum. Grup sayımızın 16 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.***

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

Farklı gruplarda bulunan Nessus tarama aracı üzerine çalışan ekiplerle birleştikten sonra tarama sonuçlarından çıkan riskleri araştırmak üzere risklerin dağıtımı yapıldı. ***Ben TLS Versiyon 1.0 ve 1.1 kullanımının orta derece risk barındırdığından araştırmasını yaptım.***

Yaptığım Tarama ve Araştırmalar

1. Nessus Kurulumu
2. Nessus ile Basic Network Scan
3. Nessus Sunumu (Tarama işlemi kısmından soru-cevap)
4. Tarama Araçları ile Yapılan Taramaların Rapor Sunumu Hazırlığı
5. Genel Raporun İçerisinde Bulunan Nessus Sunumu
6. Nessus Ekiplerinin Birleşimi Sonrası TLS Versiyon Riski Araştırması

1. Nessus Kurulumu

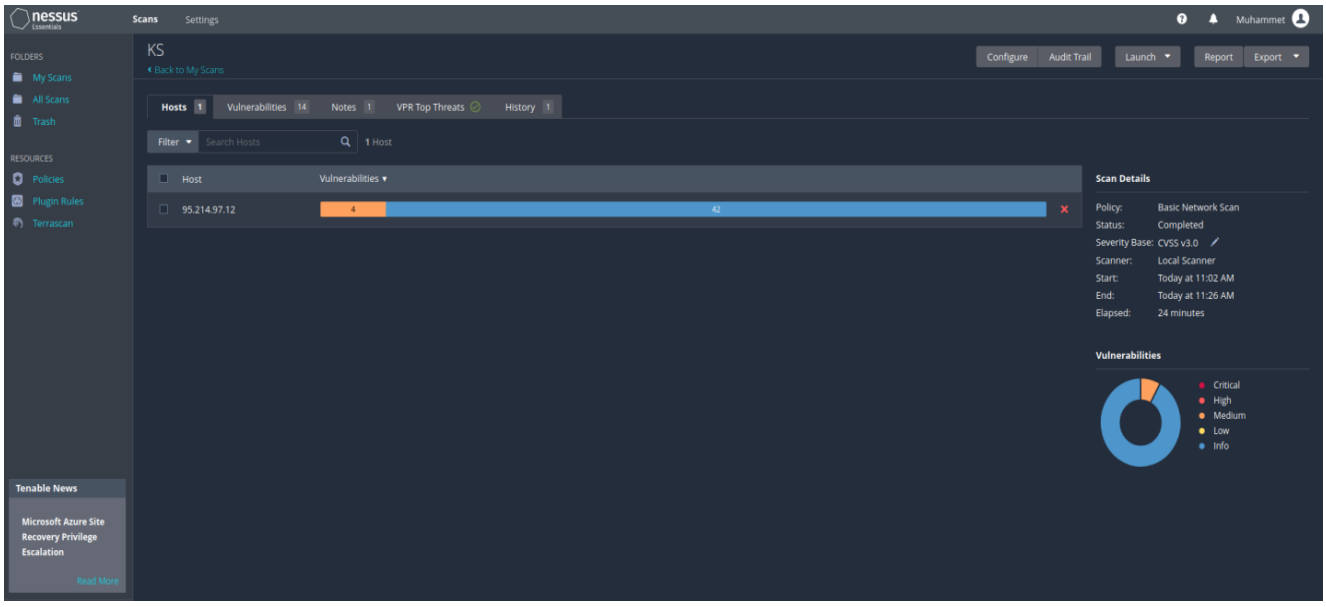
https://www.tenable.com/downloads/nessus?loginAttempted=true linki üzerinden Nessus kurulum dosyasının indirmesini yapıyoruz. İndirdiğimiz kurulum dosyasını sanal makine ile kullandığım Kali'nin içerisine attıktan sonra terminal kısmına:

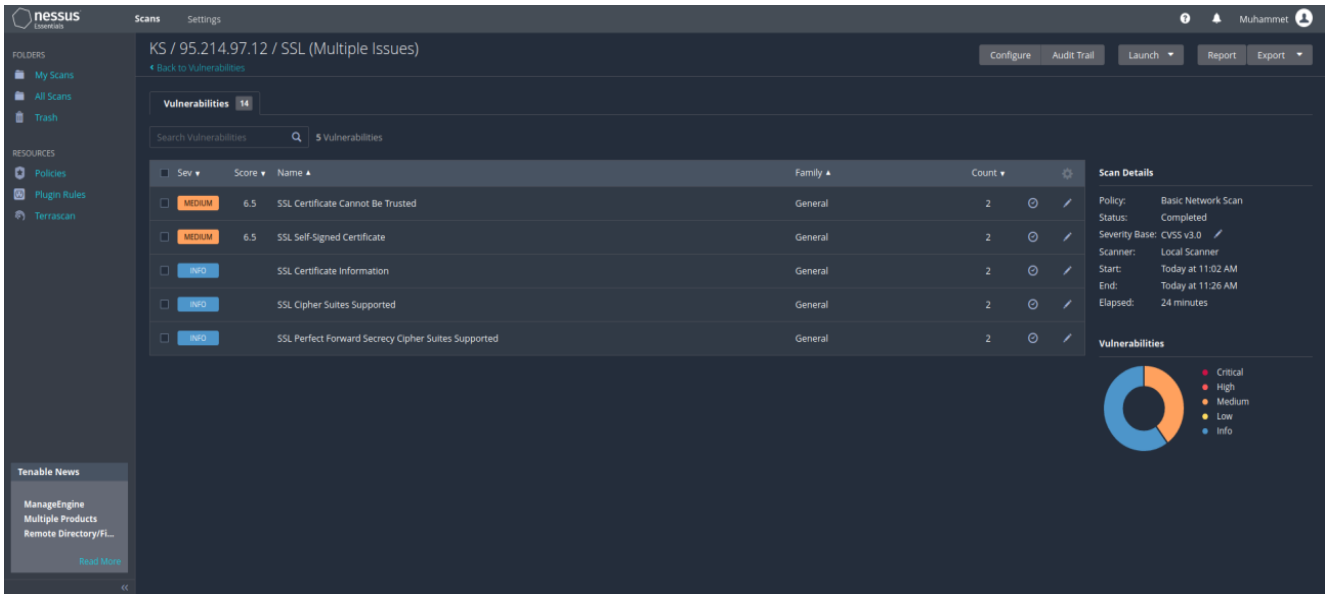
- ➔ Cd (Kurumlum dosyasının bulunduğu konumu yazıyoruz örneğin;) Desktop
- ➔ Sudo dpkg -i "kurulum dosyası ismi"(Nessus-8.11.1-debian6_amd64.deb)
- ➔ /bin/systemctl start nessusd.service (Kurulum bittikten sonra bu komut ile birlikte Nessus'u çalıştırıyoruz)
- ➔ (Daha sonra tarayıcı üzerinde Nessus tarama aracını açıyoruz) https://kali:8834/

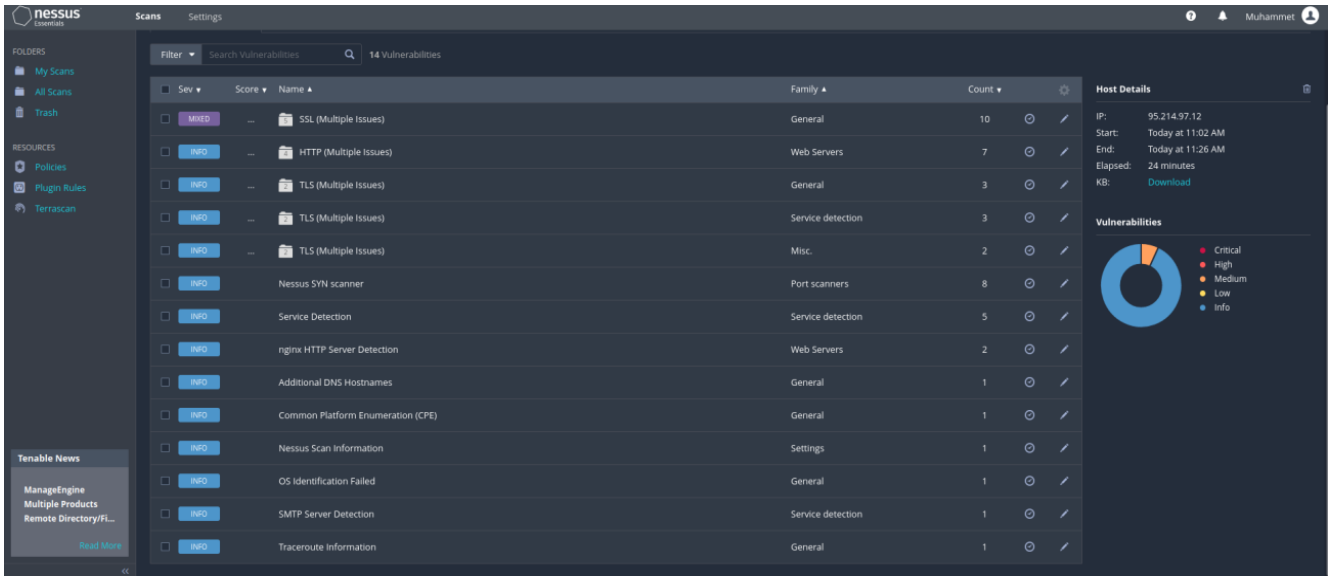
2. Nessus ile Basic Network Scan

Tarama işlemi için daha öncesinde saldırı yapıldığını bildiğim ve taraftarı olduğum Kocaelispor kurumsal web sitesinin taramasını yaptım.

Tarama Sonuçları







3. Nessus Sunumu (Tarama işlemi kısmından soru-cevap)

Nessus tanıtımını yaparken tarama kısmında eğitmenden gelen sorulara yanıtlama yaptım.

Soru: Bulduğunuz riskler nasıl kullanılabilir?

Cevap: Portların açık olması güvenlik zafiyeti oluşturabilir. Yapılan önceki saldırılar görülebilir ve bilgi edinebilir. Ddos saldırısı yapılabilir.

SSL sertifikasının kendinden imzalı olması maliyetten kaçıp güvenlikten ödün vermektedir.

4. Tarama Araçları ile Yapılan Taramaların Sunum Hazırlığı

Araçların hepsi ile Muş Ticaret ve Sanayi Odası tarama yapıldıktan sonra raporları birleştirip düzenleme görevini üstlendim. Son çıktıların powerpoint sunumunu hazırladım.

5. Genel Raporun İçerisinde Bulunan Nessus Sunumu

Yaptığımız genel raporlama sonrasında Nessus sunumu noktasında kimsenin sunumu üstlenmemesi sonrası sunmak durumunda kaldım. Sunum sonrasında başka tarama araçları noktasında da soruları yanıtladım.

6. Nessus Ekiplerinin Birleşimi Sonrası TLS Versiyon Riski Araştırması

Genel rapor sonrası eğitmenimizin daha olgun ve detaylı sonuç alabilmek için aynı tarama araçlarını ve aynı kurumu tarayan ekiplerin birleşimini uygun gördü. Nessus kullanan ve Muş Ticaret ve Sanayi Odasını tarayan ekiplerle birleştikten sonra 1. Grubun yapmış olduğu tarama sonucu aldığı riskler üzerinden görev dağılımı yapıldı. TLS Versiyon 1.0 ve 1.1 kullanımın neden risk teşkil ettiği ve nasıl giderileceğine dair 2 kişiyle birlikte görevlendirildik.

Araştırmalarımız sonucu TLS 1.0 ve 1.1 versiyonun artık kullanılmadığı ve bu versiyon kullanımlarının ciddi sorunlar oluşturabileceğini tespit ettik. Çözüm olarak ise TLS versiyon 1.2 veya 1.3'e yükseltilmesi gerektiğini karar kıldık.

TLS versiyonlarının sürümlerinin saldırılara karşı şifreleme güvenliğinin yeterliliği ile alakalı wikipedia.org kaynaklı tabloyu aşağıda bulundurdum.

Bilinen uygulanabilir saldırılara karşı şifreleme güvenliği

Şifreleme			Protokol versiyonu					Durum
Tip	**Algoritma**	**Güç (bits)**	**SSL 2.0**	**SSL 3.0** [n 1][n 2][n 3][n 4]	**TLS 1.0** [n 1][n 3]	**TLS 1.1** [n 1]	**TLS 1.2** [n 1]	
Block cipher mode of operation	AES GCM[n 5]	256, 128	Yok	Yok	Yok	Yok	Güvenli	RFC'lerde TLS 1.2 için tanımlanmıştır
	AES CCM[n 5]		Yok	Yok	Yok	Yok	Güvenli	
	AES CBC[n 6]		Yok	Yok	Alınan önlemlere göre değişir	Güvenli	Güvenli	
	Camellia GCM[n 5]	256, 128	Yok	Yok	Yok	Yok	Güvenli	
	Camellia CBC[n 6]		Yok	Yok	Alınan önlemlere göre değişir	Güvenli	Güvenli	
	ARIA GCM[n 5]	256, 128	Yok	Yok	Yok	Yok	Güvenli	
	ARIA CBC[n 6]		Yok	Yok	Alınan önlemlere göre değişir	Güvenli	Güvenli	
	SEED CBC[n 6]	128	Yok	Yok	Alınan önlemlere göre değişir	Güvenli	Güvenli	
	3DES EDE CBC[n 6]	112[n 7]	Güvensiz	Güvensiz	Az güçlü, Alınan önlemlere göre değişir	Az güçlü	Az güçlü	
	GOST 28147-89 CNT	256	Yok	Yok	Güvenli	Güvenli	Güvenli	RFC taslaklarında önerilmiştir
	IDEA CBC[n 6][n 8]	128	Güvensiz	Güvensiz	Depends on mitigations	Güvenli	Yok	TLS 1.2'den kaldırılmıştır
	DES CBC[n 6][n 8]	56	Güvensiz	Güvensiz	Güvensiz	Güvensiz	Yok	
		40	Güvensiz	Güvensiz	Güvensiz	Yok	Yok	TLS 1.1 ve sonrası için yasaklanmıştır
	RC2 CBC[n 6]	40	Güvensiz	Güvensiz	Güvensiz	Yok	Yok	
Stream cipher	ChaCha20-Poly1305[n 5]	256	Yok	Yok	Yok	Yok	Güvenli	RFC taslaklarında önerilmiştir
	RC4[n 9]	128	Güvensiz	Güvensiz	Güvensiz	Güvensiz	Güvensiz	TLS'nin tüm versiyonları için yasaklanmıştır
		40	Güvensiz	Güvensiz	Güvensiz	Yok	Yok	
None	**Null**[n 10]	-	Yok	Güvensiz	Güvensiz	Güvensiz	Güvensiz	RFC'lerde TLS 1.2 için tanımlanmıştır

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.