Bilgi Sistemleri ve Güvenliği Dersi
Bireysel Rapor

170541045
Ahmet Furkan Bozkurt

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.

Bilgi güvenliğinin amacı ve öneminin kazanımlarını sağladığım bir ders oldu,Farklı bir işletim sistemi olan Kali ile tanışmış oldum , ayrıca zafiyet taraması ve sızma yöntemlerini öğrendim.

Özet

1 numaralı grup içerisinde araştırma ve swot analizi gibi bazı konuları üstlendim
Bir çok farklı kaynaktan Nesus ile ilgili araştırmalar yaptım sadece kaynaklarla yetinmeyip daha önce Nesus kullanmış kişilerden de fikirler alarak bir swot analizi ortaya koydum ve ekip arkadaşlarımla paylaştım

Nesus Nedir güçlü,zayıf yönleri nelerdir araştırılıması, tarama işlemi ve Sunumun hazırlanmasında ekibi organize etme

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

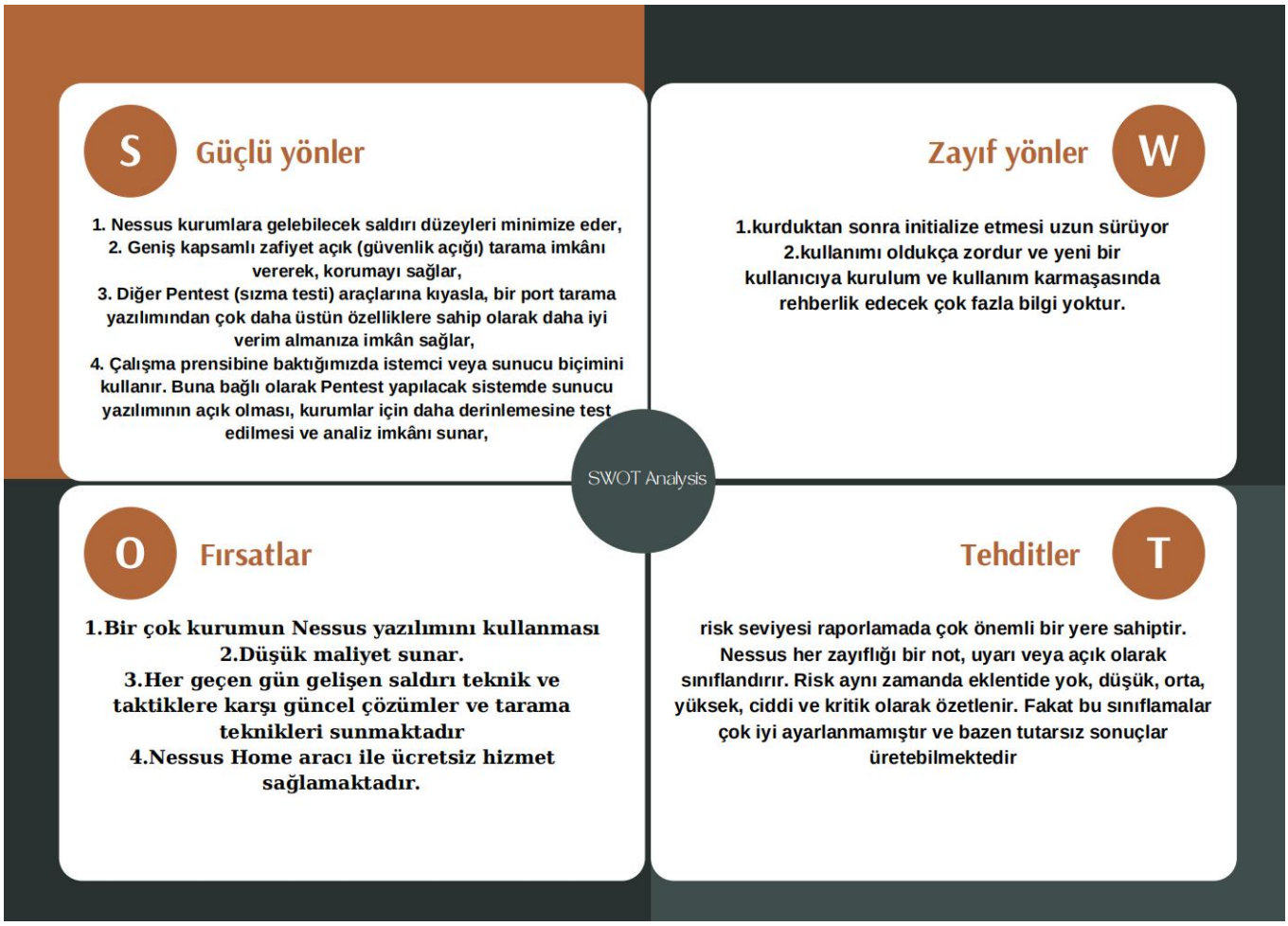
Farklı gruplarda bulunan Nessus tarama aracı üzerine çalışan ekiplerle birleştikten sonra tarama sonuçlarından çıkan riskleri araştırmak üzere risklerin dağıtımı yapıldı. *Ben ve Muhammet arkadaşım TLS Versiyon 1.0 ve 1.1 kullanımının orta derece risk barındırdığından araştırmasını yaptım.*

Yaptığım Tarama ve Araştırmalar

1. Nessus Swot analizi
2. Tarama Araçları ile Yapılan Taramaların Rapor Sunumu Hazırlığı
3. Ekiplerinin Birleşimi Sonrası TLS Versiyon Riski Araştırması

1. Nesus Swot analizi

Swot analizi için sadece kaynakları değil aynı zamanda kullanıcı yorumlarınıda araştırdım hatta bizzat nesus kullanmış bir kaç arkadaşımdan fikir aldım çünkü internette hemen Nesusun güçlü veya zayıf yönlerini alatan ve kapsamlı bir kaynak yok bu yüzden daha detaylı araştırıp kendi yorumlamamla beraber bir swot analizi oluşturabildi



2. Tarama Araçları ile Yapılan Taramaların Sunum Hazırlığı

Muş Ticaret ve Sanayi Odası tarama yapıldıktan sonra raporlara katkılar sağladım.

3. 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

Bilgi Sistemleri ve Güvenliği dersinden elde ettiğim sonuçlar:

- Bilgi güvenliği nedir, bilgi güvenliği araçları nedir. Artık bunlar hakkında bilgi sahibiyim
- Şuan halen devam ettiğim iş hayatında Belki bilgi güvenliği işi yapmamaktayım ama artık hiç değilse iş hayatımda bana elbet birgün yarayacağını düşündüğüm tecrübeler edinmiş oldum
- Penetrasyon testi kısmında ise yaptığımız laboratuvar uygulamaları, grup çalışmaları ve tarama araçlarının kullanımı ile oldukça verim aldım ve kendimi geliştirdim.
- Ekip ile çalışmasının zaten mevcut işimde deneyimlemiş biri olarak işimden kalan fazla zamanlarda ekibe kendi iş hayatımdaki ekip tecrübelerimi aktararak ekib kurrabilmeyide deneyimlemiş oldum..
- 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.