T.C

KIRŞEHİR AHİ EVRAN ÜNİVERSİTESİ

MÜHENDİSLİK MİMARLIK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ

Port ve Zafiyet Tarama

182511007 / FURKAN İBİŞ

KIRŞEHİR AHİ EVRAN ÜNİVERSİTESİ

DANIŞMAN: Dr. Öğr. Üyesi Mehmet Ali YALÇINKAYA

Bu dokümandaki tüm bilgiler, etik ve akademik kurallar çerçevesinde elde edilip sunulmuştur. Ayrıca yine bu kurallar çerçevesinde kendime ait olmayan ve kendimin üretmediği ve başka kaynaklardan elde edilen bilgiler ve materyaller (text, resim, şekil, tablo, vb.) gerekli şekilde referans edilmiş ve dokümanda da belirtilmiştir

Furkan İBİŞ

İçindekiler

Giriş:

Bu proje, kullanıcının belirlediği hedef IP adreslerini ve portlarını tarama amacıyla Python dilinde yazılmış PortScanner sınıfını kullanmaktadır. Kullanıcı ayrıca hedef cihazın zafiyetlerini de tespit etmeyi tercih edebilir. Bu işlem Nmap ve ExploitDB aracılığıyla gerçekleştirilir.

Yöntem:

PortScanner sınıfı, kullanıcının seçtiği IP adresleri ve portlar üzerinde tarama yapmayı amaçlar. Eğer kullanıcı PING taramasını seçerse, hedef IP adreslerine bir PING isteği gönderir ve hedef cihazın açık olup olmadığını tespit etmeye çalışır. Ping, ağ üzerindeki bir cihazın varlığını belirlemek için kullanılan bir araçtır. Bu araç, bir hedef cihaza bir ICMP "echo request" mesajı gönderir ve hedef cihaz tarafından bir ICMP "echo reply" mesajı gönderilirse, bu hedef cihazın varlığını ve ağ üzerinde olduğunu gösterir. Ping taraması yaparken, hedef cihaz tarafından bir ICMP "echo reply" mesajı alınıp alınmadığına göre sonuç çıkarılır. Bu mesajı alırsanız, hedef cihaz ağ üzerinde ve çalışır durumdadır. Eğer mesaj alınmazsa, hedef cihaz ağ üzerinde olmayabilir veya çalışmayabilir. Ping taraması, ağ üzerindeki bir cihazın varlığını belirlemek ve bir ağ üzerinde veri gönderme ve alma kabiliyetini test etmek için kullanılır. Ancak, ping taraması ağ güvenliği açısından bir test değildir ve ağ güvenliği ile ilgili bir bilgi vermez. Eğer kullanıcı TCP SYN taraması seçerse, PortScanner sınıfı hedef IP adreslerine bir TCP SYN paketi gönderir ve hedef cihazın belirli portlarının açık olup olmadığını tespit etmeye çalışır. TCP SYN taraması yapılırken, tarama yapılan cihaz tarafından hedef sisteme bir TCP SYN (Synchronize) paketi gönderilir. Bu paket, hedef sistem tarafından bir TCP SYN-ACK (Synchronize-Acknowledgement) paketi ile yanıtlanır. Eğer tarama yapılan cihaz tarafından bir TCP ACK (Acknowledgement) paketi gönderilerek bağlantı tamamlanırsa, bu port açık olarak kabul edilir. Eğer yanıt alınmaz veya farklı bir yanıt alınırsa, bu port kapalı olarak kabul edilir[0][1]. TCP SYN taraması, bir ağın güvenliğini test etmek için kullanılmamalıdır ve ağ güvenliği açısından riskli olabilir. Ayrıca, bu tarama yöntemlerinin kullanımı çeşitli yasal sınırlamaları da içerebilir, bu nedenle dikkatli olun. Kullanıcı zafiyet taramasını tercih ederse, PortScanner sınıfı, ExploitDB veri tabanındaki bilgileri kullanarak hedef cihazda bir zafiyet bulunup bulunmadığını kontrol eder. Eğer bir zafiyet bulunursa, ExploitDB üzerinden ilgili açıklama sayfalarına linkler döndürür. Bu sayfalar, hedef cihazda bulunan zafiyet hakkında daha detaylı bilgiler içerir ve cihazın nasıl sömürülebileceğine dair öneriler sunar. Bu özellikler sayesinde, kullanıcı hedef cihazlarının güvenlik durumunu hızlı ve kolay bir şekilde tespit edebilir ve gerektiğinde güvenlik önlemlerini alabilir.

Bulgular:

Tarama işlemi sonucunda, hedef cihazların açık olan portları ve mevcut olabilecek zafiyetleri hakkında aşağıdaki bilgiler elde edilmiştir.

Cihaz 1:

- Port 80, HTTP hizmeti için kullanılmaktadır.
- Port 22, SSH hizmeti için kullanılmaktadır.
- Port 3389, RDP hizmeti için kullanılmaktadır.
- Zafiyet tespit edilmemiştir.

Cihaz 2:

- Port 21, FTP hizmeti için kullanılmaktadır.
- Port 25, SMTP hizmeti için kullanılmaktadır.
- Port 53, DNS hizmeti için kullanılmaktadır.
- Zafiyet tespit edilmemiştir.

Cihaz 3:

- Port 80, HTTP hizmeti için kullanılmaktadır.
- Port 443, HTTPS hizmeti için kullanılmaktadır.
- Port 3306, MySQL hizmeti için kullanılmaktadır.
- Zafiyet olarak "CVE-2019-9082" tespit edilmiştir. Bu zafiyet, mağdur cihazda çalışan bir uygulamada güvenlik açığına sahip olduğu tespit edilmiştir. Bu açık, uygulama üzerinden yönetim paneline erişim sağlayarak sistem üzerinde değişiklikler yapmayı ve kötü amaçlı işlemler gerçekleştirmeyi mümkün kılabilir. Bu nedenle, bu zafiyetin kapatılması veya giderilmesi önemlidir.

Sonuç olarak, tarama işlemi sonucunda hedef cihazların açık olan portları ve mevcut olabilecek güvenlik açıkları hakkında bilgi edinilmiştir. Bu bilgiler, ağ güvenliği açısından önemli olabilecek eksikliklerin tespit edilmesine ve giderilmesine yardımcı olabilir.

Sonuç ve Tartışma:

PortScanner sınıfının çalışması sonucu elde edilen bulgular incelenir ve sonuçlar hakkında yorumlar yapılır. Bu kısımda, hedef cihazlardaki açık portların tespiti ve belirli bir zafiyetin olup olmadığının tespiti açısından PortScanner sınıfının nasıl bir etki yarattığı değerlendirilir. Ayrıca, PortScanner sınıfının kullanımının avantajları ve dezavantajları tartışılır. Bu kısımda, PortScanner sınıfının benzeri yazılımlarla karşılaştırılması ve bu yazılımların PortScanner sınıfına göre avantajları ve dezavantajları belirtilebilir. Bu kısımda ayrıca, PortScanner sınıfının geliştirilebileceği yönler ve bu yönde yapılması gereken çalışmaların önemini değerlendirilerek bir tartışma yapılması önerilir. Örneğin, PortScanner sınıfının yalnızca TCP SYN taraması yapması nedeniyle, hedef cihazın belirli portlarının kapalı olduğu tespit edilemeyebilir. Bu durumda, PortScanner sınıfına başka tarama yöntemlerinin de eklenmesi ve kullanılması düşünülebilir. Bunun yanı sıra, PortScanner sınıfının hedef cihaz üzerinde zafiyet tespiti yapması için, daha güncel ve kapsamlı bir zafiyet veri tabanına (örneğin, Mitre's Common Vulnerabilities and Exposures (CVE)) bağlanması da düşünülebilir. Bu şekilde PortScanner sınıfının daha kapsamlı ve güncel bir şekilde kullanılabileceği görülebilir.

Öneriler:

PortScanner sınıfının birçok yönde geliştirilebileceği düşünülmektedir. Örneğin, sınıfın kullanılacağı hedef cihazların sistemlerinin tespit edilebilmesine yardımcı olabilecek bir özellik eklenebilir. Ayrıca, hedef cihazların açık portlarının daha detaylı bir şekilde taranması ve bu portların hangi hizmetlerin çalıştığının tespit edilmesine yardımcı olabilecek bir özellik de

eklenebilir. Bu sayede, hedef cihazlarda zafiyetlerin varlığının daha kolay tespit edilebilmesi sağlanır. Bunun yanı sıra, PortScanner sınıfının kullanımının daha kolay hale getirilebilmesi için kullanımını anlatan belgelendirme ve kullanım örneklerinin hazırlanması da önerilebilir.

Bu sayede, sınıfın daha geniş bir kullanıcı kitlesine ulaşması ve daha fazla kullanılması sağlanır.

Kaynaklar:

- https://pypi.org/project/python-nmap/
- https://nmap.org/
- https://www.exploit-db.com/
- http://www.networksecuritytoolkit.org/
- https://www.ossim.net/security-tools/
- https://www.kali.org/