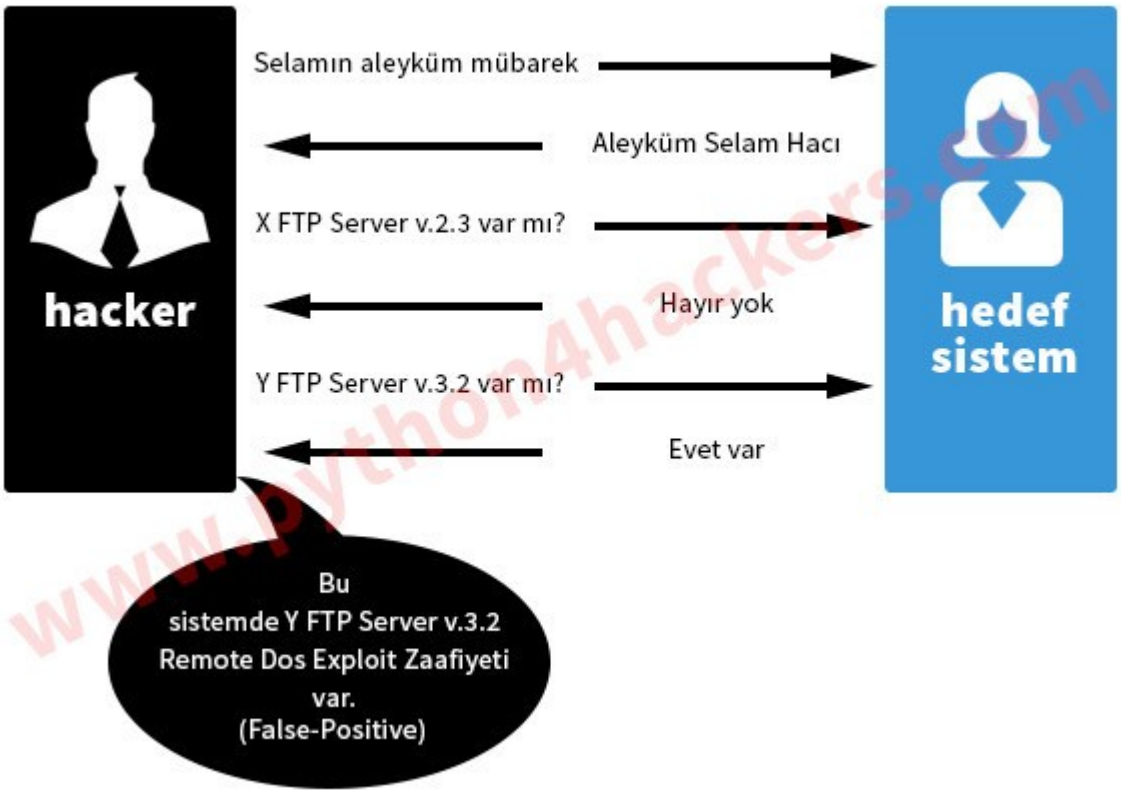
Vulnerability Scanner'ların Çalışma Mantığı

Vulnerability Scanner'lar hedef sistemi tararken öncelikle port taraması yaparak hedef sistemin açık veya filtreli portlarını keşfederler. Eğer açık portlarda yer alan servis bilgilerini sezebilirlerse veyahut keşfedebilirlerse daha sonra Scanner'ın kendi veritabanında yer alan güvenlik zafiyetli servislerin isimleriyle keşfedilen servisin ismini karşılaştırırlar. Eğer eşleşme gerçekleşirse bu sistemde servisin adıyla anılan atıyorum XYZ zafiyeti var derler. Fakat Vulnerability Scanner'lar keşfedilen zafiyetin sistemde gerçekten var olup olmadığını doğrulayamazlar. Sadece bir ihtimal, belki kuvvetle muhtemel var derler. Aşağıda Vulnerability Scanner'ların ilgili port'ta servis tespit etme konusunda bir analojik yaklaşımı görmektesiniz:



Evet, belki hedef sistemin bir portunda çalışan Y servisinde Vulnerability Scanner'ın tespit ettiği gibi bir zafiyet var olabilir. Fakat daha önceden güvenlik uzmanları tarafından bu zafiyet kapatılmış olabilir (fix'lenmiş olabilir) Veyayut serviste açık vardır, fakat düzgün çalışmıyordur. İşte bu ve bunun gibi nedenlerden ötürü Vulnerability Scanner'lar tarafından keşfedilen zafiyetlerin durumuna “False-Positive” denmektedir. Yukarıdaki resimde varılan sonuç bir False-Positive örneğini teşkil etmektedir.

http://python4hackers.com/python-network-hacking-tools/vulnerability-assessment-tarayicilarinin-calisma-mantigi.html