CEH mi yoksa OSCP mi ?

written by Mert SARICA | 15 December 2009
If you are looking for an English version of this article, please visit here.

2005 yılının başlarında Altunizade'deki bir eğitim kurumunda EC-Council'in CEH eğitimini almaya karar vermiştim ve bu kurstan beklentilerimde oldukça yüksekti. Normalde yurt dışında 5 günde verilen bu eğitimi yanlış hatırlamıyorsam 3 aylık bir kursa çevirip vermişlerdi. Bu kursta yazılımlarda nasıl güvenlik açığı bulunacağını ve istismar edilebileceğini ve istismar uygulamasının nasıl geliştirileceğinin öğretileceğini bu sayede bilgilerimi pekiştirebileceğimi düşünüyordum ancak ne zamanki günün birinde winnuke programının nasıl kullanılacağı gösterilmiş ve eğitmen tarafından beklentilerimi aşağıya çekmem gerektiği belirtilmişti, işte o zaman bu kursun bana pek fazla katkısı olmayacağını anlamıştım. Aslında bakıldığında eğitim materyallerinde exploit writing, reverse engineering gibi keyifli modüller olmasına rağmen kursta bu modüller işlenmiyordu sebebi ise EC-Council'in 22 ile 26 arasındaki modüllerin self-study olmasına karar vermesinden kaynaklanıyordu. Yanlış hatırlamıyorsam o zamanki CEH sürümü v4 idi (2003) ve kursun başlarında v5 (2005) çıktığı için eğitim materyallerimiz güncellenmişti. Sertifikaya sahip olmak içinse çoktan seçmeli bir sınavdan başarıyla geçmeniz gerekiyordu (halende öyle sanırım).

Yıllarca eğitim içeriğinin zayıf olması, internetten indirilebilen sınav soruları ve cevapları ile sahip olunabilecek ve teorik bilgiye dayalı bir sınav sisteminin olması nedeniyle bu eğitim ve sertifika hakkında olumsuz görüşlerde bulunuyordum. Sınav sistemi bir kenara eğitim içeriği ethical hacking konusunda hiç bir bilgisi olmayan, başlangıç seviyesindeki kişiler için faydalı olabilirdi, belkide eğitimden beklentilerim yüksek olduğu için beni hayal kırıklığına uğratmıştı.

Aradan yıllar geçti ve geçtiğimiz yıl, sanıyorumki Haziran ayının başlarıydı, v6 piyasaya çıktı. İçeriğine bakıldığında v5'te 26 modül varken v6 67 modülden oluşuyor ve içeriği 2005 yılına kıyasla oldukça tatminkar ancak v5'te olduğu gibi en keyifli ve bilgilendirici modüller kursun bir parçası olarak katılımcılara gösterilmiyor. (1-21 arası modüller zorunlu geri kalanlar ise self-study)

Yaptığım iş gereği insanların çoğunun sorduğu ilk soru CEH sertifikasına sahip olup olmadığımdı. Yıllarca bıkmadan usanmadan yukarıdaki nedenlerden

ötürü neden CEH sertifikasına sahip olmadığımı anlattım durdum ve bu yılın başında bu soruya yanıt olması açısından ethical hacking eğitimi ve sertifikası üzerine yaptığım araştırmalar sonucunda içeriğinin ve sınav sisteminin beni oldukça tatmin ettiği bir eğitim ile karşılaştım, Offensive Security 101 yeni adıyla Penetration Testing with Backtrack. Adından da anlaşılacağı üzere Backtrack'in yapımcıları tarafından hazırlanmış ve isterseniz yurt dışında isterseniz online olarak alabileceğiniz bir eğitim. Eğitimi internet üzerinden almanız durumunda pdf formatında olan eğitim materyalini okuyabiliyor, pratik bilgiler içeren video formatındaki modülleri izleyebililiyor ve öğrendiklerinizi pratiğe dökmenize olanak sağlayan sunucularına vpn erişimi ile bağlanabiliyorsunuz. Fuzzing ile güvenlik açığı keşfetmekten, python ile istismar uygulaması hazırlamaya, ollydbg ile return adresi bulmaya kadar CEH'e kıyasla ileri düzeyde bilgi edinmenizi sağlıyor. Sınav sistemi ise CEH ile kıyaslanamaz nedeni ise tamamen pratiğe dayalı olması, sınav günü size sınav ortamına erişebilmeniz için vpn tanımları yapılıyor ve yanlış hatırlamıyorsam 4 soru veriliyordu. Bir soruda sizden bir uygulamadaki buffer overflow güvenlik zafiyetini araştırmanızı ve uzaktan kod çalıştırmanıza imkan tanıyan istismar uygulamasını yazmanızı isterken diğer bir soruda labdaki linux sunucuyu ele geçirmenizi ve root klasörü altındaki text dosyası içerisinde yer alan satırı kendilerine iletmeniz isteniyor ve bunları gerçekleştirirken otomatik tarama araçlarından (nessus, core impact) faydalanmanız yasak, kısacası eğitim içeriğinden sınavına kadar oldukça başarılı olduğunu söyleyebilirim.

Sonuç olarak yolun başındaysanız, ethical hacking konusundaki bilgi düzeyiniz az ise, eğitimi verecek eğitmen işinin ehli ise (pentester olması kesinlikle tercih sebebi olmalıdır), zaman zaman ders programının dışına çıkabilecek hatta self-study olan modülleride eğitimde işleyebilecek ise (EC-Council buna imkan tanıyor mu bir fikrim yok) CEH eğitimini ve sertifikasını (vasat sınav sistemi nedeniyle eğitim ilede yetinebilirsiniz) önerebilirim. Ancak ethical hacking konusunda az çok bir bilgiye sahipseniz ve bunu pratiğe dökerek sertifikalandırmak istiyorsanız OSCP eğitimini ve sertifikasını şiddetle öneririm.