Nasıl Ahlaklı Korsan Olunur ?

written by Mert SARICA | 19 May 2011

Bu soruyu kendime ilk sorduğumda 15-16 yaşlarındaydım. Google arama motorunun var olduğu ama bilinmediği o yıllarda Altavista arama motoru ile bu soruya yanıt aramak ve cevabını içeren sayısız kaynağa ulaşmak pek mümkün olmuyordu bu nedenle benim de yolum o zamanlar kullanımı oldukça popüler olan IRC sunucularından geçti. EFnet IRC Ağı'nda yer alan #Hackers kanalında sabah akşam konuşmaları takip ederek az da olsa birşeyler öğrenmeye çalışıyordum. Günün birinde sohbet ettiğim bir kişi (keşke rumuzunu hatırlayıp teşekkür edebilsem) samimi bir şekilde programlama konusunda bilgi sahibi olmam gerektiğini ve işletim sistemi olarak sadece Windows ile yetinmeyerek Linux işletim sistemi de kullanmam gerektiğini söylemişti. Programlama kısmını anlıyordum ancak kara kuru bir ekranda çalışmanın bana ne gibi bir getirisi olacağı konusunda şüphelerim vardı. Aradan 15 sene geçtikten ve ahlaklı korsan (ethical hacker, penetration tester) olduktan sonra ne zaman program yazsam kendi kendime adam haklıymış der, ne zaman Backtrack ile çalışmam gerekse al sana kara kuru ekran der dururum :)

Ne mutlu bana ki dünyanın 4 bir yanından, özellikle genç arkadaşlardan çok sayıda e-postalar alıyor ve her birini özenle yanıtlıyorum. Çoğunun yanıtını aradığı tek bir soru var, nasıl ahlaklı korsan olurum, nereden ve nasıl başlamalıyım?

Öncelikle yazımı ahlaksız korsanların okuması ihtimaline karşı neden ahlaklı olunması gerektiği konusunu kısaca bir kaç madde ile açıklayayım.

- Yasalar ile başınız derde girmez.
- Bu işi kariyere dönüştürerek uzun vadede para kazanabilirsiniz.
- İnsanların güvenini, sevgisini ve saygısını kazanabilirsiniz.
- İşvereninizin desteğini arkanıza alarak pahalı eğitimlere, konferanslara bedava katılma şansı yakalayabilirsiniz :)

Gelelim ahlaklı korsan olmak için yapmanız gerekenlere;

- İngilizce öğrenin: Herşeyden önce İngilizce bilmeniz gerekir en azından okuduğunuzu anlayacak kadar diyelim. Nedeni basit, güvenlik sektöründe gerçekleştirilen çalışmalardan, kaynaklara kadar çoğu materyalin dili

İngilizce bu nedenle gündemi, gelişmeleri yakından takip edebilmek için ne yapın ne edin öncelikle İngilizce öğrenmeye bakın, olmazsa olmaz.

- Programlama dili öğrenin: Hacker'ın İngilizce sözlük anlamına bakacak olursanız programcı kelimesinin geçtiğini görebilirsiniz. Korsan olupta programlama bilmemek gibi bir şansınız yok, yok diyenlerede itibar etmeyin. İstismar aracı hazırlamayı bir kenara koydum en azından kısa zamanda çok iş başarabilmek ve bunu otomatiğe bağlayabilmek için kendi programınızı yazmanız gereken zamanlar mutlaka olacaktır. Teknik olarak ileri seviyeye ilerledikçe (misal tersine mühendislik yaparken) programlamanın şart olduğunu görebilirsiniz. Güvenlik zafiyeti keşfedebilmek için C programlama dilini öğrenmeniz gerekecektir. Bu dil sayesinde diğer programlama dillerini okuduğunuzda rahatlıkla anlayabildiğinizi göreceksiniz bu sayede kaynak kodu analizi sizin için daha kolay olacaktır. Testler esnasında işinizi kolaylaştıracak dillerden bir tanesini muhakkak öğrenmelisiniz. Bunun için Python'u tercih ettim, mutluyum, huzurluyum. Kapalı kaynak kodlu yazılımlarda güvenlik zafiyeti keşfetmekten istismar kodu, kabuk kodu oluşturmaya kadar bir çok aşamada Assembly programlama dilini biliyor olmanız yararınıza olacaktır. Metasploit ve diğer araçlar ile hepsini hallederim demeyin, başlangıç seviyesinden öteye gidemez, program bağımlı yaşarsınız.
- Bol bol okuyun ve pratik yapın: Ağ, sistem, veritabanı, web uygulaması konularında temel kitaplar okuyun ve bilgi seviyenizi arttırın. Temel seviyede bilgi sahibi olduktan sonra tüm bu alanlar ve daha fazlası ile ilgili hacking kitapları okumaya başlayın. Bunun için Amazon.com sitesine giderek hacking anahtar kelimesi ile sorgular yapın ve en çok okunan, beğenilen kitapları sırayla okumaya başlayın. Başlangıç seviyesi için Hacking Exposed serilerini önerebilirim. Okuduğunuzu pratik etmezseniz unutmanız ve ihtiyaç duymanız durumunda tekrar okumanız gerekebileceği için kendinize windows ve linux işletim sistemleri kurulu iki sanal makina oluşturun ve tüm denemelerinizi, öğrendiklerinizi bu sistemler üzerinde gerçekleştirerek pratiğe dökün.
- Sertifika alın ve eğitimlere gidin: Kim ne derse desin sertifikalar işe girmenizi kolaylaştırmaktadır. Sertifikayı kartvizit olarak düşünebilirsiniz. Karşı tarafın (işveren, iletişim kurduğunuz kişiler vs.) spesifik olarak belli bir alanda sertifikalandırabilecek düzeyde temel bilgi seviyesine sahip olduğunuzu anlamasına yardımcı olacaktır. Tehditler, riskler ve sürekli değişen saldırı yöntemlerini göz önünde bulundurduğunuzda kendinizi sürekli güncel tutmanız gerekiyor ve

katılacağınız eğitimler kitaplara kıyasla kısa zamanda bu bilgiyi almanızı sağlamaktadırlar. (Maddi olanakları çok fazla dert etmeyin çünkü kurumsal bir firmada çalışıyorsanız eğitime bedava gidebileceksiniz.)

- Sabırlı ve duyarlı olun: Bir güvenlik zafiyeti keşfettiğiniz zaman (karşı sisteme saldırarak değil!) örnek olarak kullandığınız bir hizmet tasarımsal olarak güvenli değil veya kullandığınız programda güvenlik zafiyeti keşfettiniz yapacağınız ilk iş zafiyetin doğru, geçerli olduğunu teyit etmek olmalıdır. Emin olduktan sonra responsible disclosure modelini izleyerek sistemin yetkilisi veya programın dağıtıcısı ile görüşerek durumu izah etmeye çalışın. Empati yaparak kendinizi karşı tarafın yerine koyun ve amacınızın güvenlik zafiyetini ortadan kaldırmak olduğunu ve bu hizmeti veya programı kullanan kişilerin art niyetli kişiler tarafından istismar edilmesini engellemek olduğunu ve bu nedenle karşı taraf ile iletişime geçtiğinizi aklınızdan çıkartmayarak karşı taraf ile şartlar ne olursa olsun işbirliği yapmaya çalışın. Responsible disclosure modelinde zafiyet ortadan kalktıktan sonra zafiyet ile ilgili detaylı bilgiye ilgili platformlarda yer verebilirsiniz eğer firma güvenlik bülteninde adının geçmesini istemiyorsa saygı duyun ve sansürleyerek yayınlayın çünkü amacımız firmayı ve hizmetlerini kötülemek değil, insanların güvenliğini sağlamak…
- Bilişim hukukundan anlayan bir avukat tutun: Responsible disclosure modelinde karşı taraf ile iletişim kurmaya çalışırsınız ancak iletişim kuramadığınız durumlarda daha doğrusu karşı taraftan herhangi bir yanıt alamadığınız durumlarda bu güvenlik zafiyetini ilgili platformlarda açıklayarak bu sistemi veya hizmeti kullanan insanları bu konuda bilgilendirir ve yetkilileri göreve çağırırsınız. Ancak kimi zaman işler istediğiniz şekilde ilerlemeyebilir ve karşı taraf e-posta atmışsın ama telefon açmamışsın diyebilir, ben 20 yıldır güvenlik sektöründeyim vay efendim sen benim kim olduğumu biliyor musun diyebilir, güvenlik zafiyetini namus meselesi yaparak sen benim namusuma nasıl el uzatırsın diyebilir, sizin onlarla onların iyiliği ve müşterilerinin güvenliği için iletişim kurmaya çalıştığınızı unutarak itibarımı zedeledin diyebilir özetle karşı taraf sizin iyi niyetinizi suistimal ederek sonunda hukuki yollara başvurabilir ve kendinizi yasalar önünde savunmanız gerekebilir. (Bugüne kadar yerli, yabancı, büyük, küçük 50’ye yakın firma ile responsible disclosure adımından geçmiş biri olarak bu ihtimalin çok düşük olduğunu ve sadece bu tür bir tavırla 1 defa

karşılaştığımı, genellikle kurumsal şirketlerde bu tür bir yaklaşımın olmadığını aksine size teşekkür edildiğini belirtmek isterim.) Bu nedenle iyi bir avukat tutmanız her zaman yerinde bir adım olacaktır.

Uzun lafın kısası ahlaklı korsan olmak için yapmanız gerekenler İngilizce bilmek, ağ, sistem, veritabanı, web uygulamaları konularında temel bilgi sahibi olmak, programlama bilmek, eğitimlere katılmak, sertifikalar almak ve bol bol hacking ile ilgili kitaplar okumak ve pratik yapmak olacaktır.

Askere gitmeden önce hazırlamış olduğum yaylalar yazı dizisinin ikincisi burada son bulurken herkese güvenli günler dilerim.