Mert Sarıca ile Hacking Üzerine [Röportaj]

8 Mayıs 2013 Çarşamba Belgeler, Güvenlik, Web Yönetimi 0

Haydar Özkömürcü

Tweetle 12 +1 4 Beğen 11

CEH ya da benzeri bir sertifika sahibi misiniz ya da bu işin bir eğitimini aldınız mı?

İşe ilk girdiğim yıl olan 2005 yılında, üniversite yönetimi tarafından Certified Ethical Hacker eğitimine gönderilmiştim fakat o zamana dek okuduğum kitaplardan ve makalelerden edindiğim bilgiler, eğitim içeriğinden çok daha ileri seviyede olduğu için eğitimin bir katma değerini ne yazık ki görememiştim.

Güvenlik ile ilgili her daim kitap okuduğum için çoğunlukla eğitimleri, sahip olduğum bilgiyi sertifikalandırmak ve CV'imde yer etmesi amacıyla kullanıyorum.

Sahip olduğum güvenlik sertifikaları CISSP, OSCP, OPST, CREA, SSCP'dir. CEH eğitimi ve sertifikasyonunun temeli, ezbere yönelik olduğu için CEH sertifikası yerine 2009 yılında, eğitimi ve sınavı pratiğe dayalı olan (hedef sistemleri hackleyerek sınavı geçebiliyorsunuz), OSCP (Offensive Security Certified Professional) sertifikasını aldım.

Hacker olmak için hep meraklı olmak gerek derler. Sizce merak yeterli mi?

2-3 yaşında anneniz, babanız size efendi efendi oynamanız için bir oyuncak alıp önünüze koyuyorsa ve siz kalkıp bunun içinde ne var diyerek canım oyuncağı kırıp, içine bakıyorsanız ve 31 yaşına geldiğinizde de mesleğiniz gereği acaba bu sistem, bu uygulama nasıl çalışıyor? nasıl hacklenir?, bu zararlı yazılım nasıl çalışıyor ? gibi sorular soruyorsanız, evet, belki de merak bu işte başarılı olmanızı sağlayan en önemli etkenlerden bir tanesidir. Tabii sadece merak, başarılı olmak için tek başına yeterli olmuyor özellikle sunum yaptığın üniversitelerde de bu işe ilgi duyan öğrenci arkadaşlara da söylediğim gibi önce merak sonra bol bol okumak ve bol bol pratik yapmak bu iş için olmazsa olmazdır.

Kendinizi "hacker" olarak mı yoksa "güvenlik uzmanı" olarak mı tanımlıyorsunuz? Ya da farklı bir tanım var mı?

Yazılı ve görsel medyada 2000 yılından bu yana değişmeyen tek şey hırlıya, hırsıza, bilene, bilmeyene hacker sıfatının yakıştırılıyor olmasıdır. Güvenlik dünyasında gerçek manada hacker, PacketStorm'dan istismar kodu indiren, derleyen ve sisteme sızan kişi değildir. Hacker, papağan dediğimiz banka kart kopyalamak için kullanılan cihaz ile banka kartı kopyalayan kişiye de denmez.

Kendinizi "hacker" olarak mı yoksa "güvenlik uzmanı" olarak mı tanımlıyorsunuz? Ya da farklı bir tanım var mı?

Yazılı ve görsel medyada 2000 yılından bu yana değişmeyen tek şey hırlıya, hırsıza, bilene, bilmeyene hacker sıfatının yakıştırılıyor olmasıdır. Güvenlik dünyasında gerçek manada hacker, PacketStorm'dan istismar kodu indiren, derleyen ve sisteme sızan kişi değildir. Hacker, papağan dediğimiz banka kart kopyalamak için kullanılan cihaz ile banka kartı kopyalayan kişiye de denmez.

Hacker, ben hackerım diyene de denmez. Benim için hacker kısaca ve kabaca programlama bilgi ve becerisine sahip, güvenlik zafiyeti keşfedebilen, istismar kodu yazabilen ve bunu gösterebilen kişiye denir. Eğer bir program ile sisteme sızabilen hacker olsaydı bugün Farmville'de tarla sürenin çiftçi, tayt ve pelerin giyenin Süperman, fare ve klavye kullanabilenin bilgisayar mühendisi, çikita muz'u yazanın da sanatçı olması gerekirdi.

13-14 yaşında rumuzunu hatırlayamadığım ancak beni doğru yönlendiren bir yabancıya, hacker nasıl olabilirim ? sorusunu sorduğumda bana verdiği cevap, C programlama dili bilmeli, ağ programlaması bilmeli ve Linux işletim sistemini kullanabilmelisin olmuştu. O yaşlarda bunları öğrenip ardından kendi güvenlik zafiyetimi keşfedip, kendi istismar kodumu yazabilir hale geldiysem ve öğrendiklerimi ve bildiklerimi insanlarla paylaşabiliyorsam, gönül rahatlığıyla kendime hacker diyebiliyorum. Ancak hacker'ın yazılı ve görsel medyada kötü olarak lanse edilmesi, bugün geldiğimiz noktada Ethical Hacker kavramının ortaya çıkmasına neden olmuştur.

Kısacası karşımdakinin farkındalığına göre kimi zaman ethical hacker'ı, kimi zaman ahlaklı korsan'ı, kimi zaman penetration tester'ı, kimi zaman ise bilişim güvenlik uzmanını kullanmaktayım.

Bir keresinde bir "güvenlik uzmanı" asla başka bir hackerı başka bir hackera övme demişti bana. Ancak yine de soracağım, sizin örnek aldığınız, hayranı olduğunuz bir hacker var mı?

VUPEN ekibinin ve Charlie Miller'ın yaptığı araştırmaları, çalışmaları oldukça beğendiğimi söyleyebilirim.

Hackerlar arasında "lamer" ve "uzman" lafları sıkça kullanılıyor. Sizce lamer'in gerçek tanımı nedir kime denir?

Bana göre lamer, sahip olduğu teknik bilgi ve beceri hacker ile aynı olmayan, başkalarının ürettiği programlara bağlı kalan, her mikrofon uzatıldığında ben hackerım diyen ama ortaya somut birşey koyamayan kişiye denir.

Mert Sarıca ile Hacking Üzerine [Röportaj]

8 Mayıs 2013 Çarşamba Belgeler, Güvenlik, Web Yönetimi 0


Haydar Özkömürcü

Tweetle 12 +1 4

Artık yasalarında iyileşmesiyle birlikte hacking haberlerini kredi kartı bilgileri vs. yerine sosyal medya üzerinden daha çok duyar olduk. Sizce Sosyal Medya'da kullanılan servisin güvenlik protokolleri dışında başka önlemler almak gerekli mi?

Belki çok klişe olacak ancak insan, güvenliğin en zayıf halkasıdır bu nedenle en temel kural, servis bağımsız olarak dikkatli ve temkinli olmak, tanımadığımız kişilerden gelen mesajları ve eklentileri açmamak olmalıdır.

Mobilin gelişmesiyle birlikte güvenlik uzmanları daha çok mobil sistemlerdeki açıklarla uğraşır oldu. Sanıyorum burada işletim sisteminin de etkisi oldukça büyük. Sizce en güvenli mobil işletim sistemi hangisi?

Mobil işletim sistemleri henüz emekleme evresinde olan işletim sistemleridir bu nedenle sıkça güvenlik zafiyetleri ile karşılaşıyor olmamızı çok yadırgamıyorum. Bugün baktığınız zaman iPhone'un Jailbreak edilmesi, bir güvenlik zafiyetinin istismar edilmesi ile oluyorsa ve bu işlem bir web sitesi üzerinden gerçekleşebiliyorsa benzer sıkıntılar Android işletim sistemi için de geçerliyse o veya bu daha güvenli demem pek doğru olmayacaktır. Ancak soruyu zararlı yazılım bulaşma riski açısından ele alırsak, Apple firması işi sıkı tuttuğu ve her uygulamayı App Store'a yüklemeden önce kaynak kod seviyesinde (code review) kontrolden geçiriyorsa fakat Google bu işi bu kadar sıkı tutmuyorsa, son kullanıcı için iPhone (iOS) daha güvenlidir diyebilirim. Bu arada yeri gelmişken, jailbreak ettiğiniz veya root yetkisi kazandığınız her cihazın, çeşitli güvenlik kontrollerini devre dışı bıraktığını dolayısıyla sizi güvenlik tehditlerine karşı korunmasız hale getirdiğini ayrıca belirtmek isterim.

Son dönemlerde sıkça telefon görüşmelerinin dinlenebilir olduğundan bahsediliyor. Dinlenemeyen telefon ya da izlenemeyen mesajlaşma uygulaması var mı?

"Akıllı telefonunuzun şarjı çabuk bitiyorsa dinleniyor olabilirsiniz" gibi söylemler bana daha çok bu işten nemalanmak isteyenlerin akılcı oyunları gibi geliyor.

Akıllı telefonlar/cihaz üzerinde uygulamalar yardımı çeşitli şifrelemeler kullanılarak görüşmelerin, mesajlaşmaların yasa dışı yollardan izlenmesi engellenebilir ancak akıllı telefonlar/cihazlar üzerinde barınan ve en yüksek yetkiye sahip olan bir casus yazılım ile teknik olarak tüm görüşmeler dinlenebilir, mesajlaşmalar izlenebilir.

DDoS saldırıları bir çok site için en sevimsiz ve en kolay gerçekleştirilebilen saldırı. Küçük siteler bu saldırılara nasıl karşı koyabilir neler önerebilirsiniz?

Geçtiğimiz ay gerçekleşen ve basına da yansıyan 300 GB büyüklüğündeki bir DDOS saldırısının CloudFlare hizmeti ile engellenmesi, küçük işletmeler, siteler için kullanılabilecek en akılcı çözüm olur diye düşünüyorum. Bkz

Mobilde ve Masaüstünde hangi antivirüs ve firewall yazılımlarını önerirsiniz?

Mobil işletim sistemleri, uygulamaları kum havuzu (Sandbox) dediğimiz kısıtlı erişime ve yetkiye sahip alanlarda çalıştırdığı için bu alanda çalışan ve en yüksek yetkiye sahip olmayan bir yazılımdan sisteminizde tam koruma sağlamasını beklemek çok gerçekçi olmaz bu nedenle mobil işletim sistemlerinde kullanılan Antivirüs yazılımlarına öncelikle çok güvenmek ve beklentiyi çok yüksek tutmak çok doğru olmayacaktır. İsimden ziyade herhangi bir antivirüs yazılımı kullanmanız yeterli olacaktır.

Masaüstü antivirüs yazılımları da baktığınız zaman ciddi bir siber saldırıda atlatılabildiği, devre dışı bırakılabildiği için yine isimden ziyade Symantec, Mcafee, Kaspersky, Eset vb. bilinen, köklü üreticilere ait antivirüs yazılımlarından birinin kullanılması faydalı olacaktır.

Sosyal Ağlarda Clickjacking, Fake Application vb. saldırılara karşı son kullanıcılara ne gibi önerileriniz olabilir?

Sosyal ağlar ve sosyal medya üzerinden gelebilecek saldırılara karşı daha önce de bahsettiğim gibi temkinli ve dikkatli olmak, şüpheli mesajları açmamak, her bağlantı adreslerine (link) tıklamamak, clickjacking vb. uygulama saldırılarına karşı Noscript gibi internet tarayıcısı eklentileri kullanmak, sahte uygulamalara karşı ise sizden istediği izinleri kontrol etmek (sizin adınıza mesaj gönderme izni, arkadaş listenizi çekme izni gibi.) yararınıza olacaktır.

Türkiye'deki hacker gruplarından biraz bahseder misiniz? Aktif olan, herkesin takip etmesi gereken gruplar hangileri?

Türk Ceza Kanunu'na ve uluslararası hukuka göre bilişim suçu işlemeyen bir hacker grubundan haberdar değilim bu nedenle bir tavsiyede bulunamayacağım.

Türkiye bugüne dek çok büyük çaplı bir siber saldırıya maruz kaldı mı?

Benim duyduğum ve/veya basına yansıyan Stuxnet, Flame ve benzeri bir siber saldırı ile henüz karşılaşmadık ancak karşılaşsaydık mevcut altyapımız ve kullandığımız teknolojiler ile bunu tespit edebilir miydik budan pek emin değilim çünkü baktığınız zaman APT (advanced persistent threat) dediğimiz "gizlen ve aksiyon al" yöntemini izleyen bu tür siber saldırılardan doğası gereği saldırısından uzunca bir zaman sonra haberdar olmaktayız.

Örneğin Kaspersky sayesinde Stuxnet'ten sonra ortaya çıkan ve siber silah olarak kullanılan Flame zararlı yazılımının Türkiye'de bir komuta kontrol merkezi olduğunu öğrendik. Gönül isterki bu tür analizleri ve tespitleri kendi yerli kaynaklarımızla yapabilelim, yerli haber kaynaklarımız ile bunlardan haberdar olabilelim.

Türkiye'de devlet kurumları siber saldırılar için ne kadar hazır?

Tatbikata ve medya üzerinden siber güvenlik bombardımanına/farkındalığına rağmen çeşitli gruplar tarafından devlet kurumları hacklenebiliyorsa ve özellikle bu saldırıların da uluslararası boyutlarda siber silahlar ile gerçekleştirilen siber saldırılar olmadığını da düşündüğümüzde hazır olduğumuzu söylemem pek doğru olmayacaktır. Umuyorum ki Tübitak bünyesinde kurulan Siber Güvenlik Enstitüsü ile siber saldırıları önlemeye, tespit etmeye ve aksiyon almaya yönelik ciddi adımlar atılacaktır.

Dünyada siber saldırılara karşı en hazırlıklı ülke hangisi?

Dışarıdan bu konuda net bir şey söylemek oldukça güç ancak gördüğüm kadarıyla Güney Kore bu konuda oldukça hazırlık yapmış. 20 Mart tarihinde Güney Kore'ye yapılan siber saldırı ile 3 banka ve 3 medya organı çalışamaz hale geldi. Baktığınız zaman 1 saat içinde hem emniyetin hem de ordunun alarm durumuna geçmesi ve soruşturma başlatması, 3 bankadan ikisinin 2 saat içinde tekrar çalışır hale gelmesi hazırlığın önemini gözler önüne sermektedir.

Mert Sarıca

Kariyer hayatım, 2003 yılında eğitim aldığım üniversitenin elektronik ders seçme uygulaması üzerinde keşfetmiş olduğum kritik güvenlik zafiyetini üniversite yönetimi ile paylaşmam ile başladı. Bu paylaşım üzerine üniversite yönetimi tarafından başarı bursu ile ödüllendirildim ve Ethical Hacker olarak işe alındım. 2006 yılında Yeditepe Üniversitesi, Bilişim Sistemleri ve Teknolojileri bölümünden mezun oldum. 2009 yılında ise Yeditepe Üniversitesi, İngilizce İşletme (MBA) programını tamamladım.

2007 yılından bu yana Finansbank'ın Bilgi Teknolojileri firması olan IBTech firmasında Senior Penetration Tester / Ethical Hacker olarak çalışmaktayım. Penetrasyon testinin yanı sıra zararlı yazılım analizi, tersine mühendislik ve adli bilişim analizi gibi bir çok alanda uzmanlaşmaktayım.