NOPcon Bilgi Güvenliği Konferansı

written by Mert SARICA | 11 May 2012

21 Mayıs 2012 Pazartesi günü NOPcon Bilgi Güvenliği Konferansı'nda, Android Uygulamalarında Güvenlik Testi konulu bir sunum gerçekleştireceğim, meraklılarına duyurulur :)

21 Mayıs 2012 Tarihinde Istanbul Bilgi Universitesi – Dolapdere kampüsünde, yerli ve yabancı alanında uzman araştırmacaların da sunumlarına yer verileceği NOPcon Bilgi Güvenliği Konferansı düzenlenecektir.

#Kimler katılmalı?
NOPcon, bilgi güvenliği/IT denetimi/network/sistem/yazılım departmanlarında ve sektöründe çalışanlara , tersine mühendislik(reverse engineering) , exploiting , vulnerability research, forensic vb hack/güvenlik konularına ilgi, merak duyan herkese hitap etmektedir.

**Katılım ücretsizdir ; http://www.nopcon.org/register/ adresinden kayıt olabilirsiniz.

#NOPcon Ana Konuları

Sınırlı kalmamakla birlikte genel olarak NOPcon sunumları aşağıdaki konuları kapsayacaktır :

Offensive Technologies (Saldırgan Güvenlik Teknolojileri):
– Exploit Geliştirme ve Bypass Mekanizmaları
– Malware
– Rootkit
– Cryptovirology

Defensive Technologies (Savunma Teknolojileri)
– Uygulama tabanlı güvenlik konuları
– Network tabanlı güvenlik konuları
– Kernel tabanlı güvenlik konuları

Embedded Device Hacking and Security (Gömülü Sistemler)
– Mobil güvenlik ve saldırı teknikleri (iphone, android, windows phone)
– Tablet, E-Reader güvenlik ve saldırı teknikleri

Vulnerability Research/Bug Hunting (Uygulama Güvenliği)
– Kaynak Kod Analizi
– Tersine Mühendislik
– Web uygulama güvenliği
– Fuzzing

Kritik Altyapı Sistemleri
– SCADA Hacking & Security
– Telekominikasyon Güvenliği
– Acil Durum Servisleri

Penetrasyon Testi için Firma Seçimi

written by Mert SARICA | 11 May 2012

Teknik yazıların yanında birazda iş hayatına, günlük işlere dair mesajlarda yazayımki verdiğim sözü yerine getirmiş olayım dedim bu nedenle bu seferki yazımda penetrasyon testi hizmeti almadan önce firma seçmek için izlediğimiz yolu sizlerle paylaşırsam faydalı olabileceğini düşündüm. Malum alacağınız hizmet penetrasyon testi olunca testi gerçekleştiren kişinin veya ekibin sertifikaları, referansları, firmanın büyüklüğü bir yana teknik olarak konuya hakimiyeti, uzmanlığı oldukça önemli bu nedenle doğru firmayı seçmeden önce mutlaka honeypot kurar ve firmaların honeypot üzerinde penetrasyon testi gerçekleştirmelerini talep ederiz.

Geçtiğimiz aylarda dört yerli bir yabancı firma ile görüştüm. Ağırlığın yerli firmalar olmasının sebebi tabiiki fiyat ve performans. Yabancı firmalar, dünyanın dört bir yanında bu hizmeti gerçekleştirmeleri nedeniyle haklı olarak geniş danışman kadrolarını, bilgi birikimlerinin fazla olmasını ve isimlerini pazarladıkları için yerli firmalara kıyasla biraz daha pahalıya bu hizmeti veriyorlar ancak günün sonunda rapora bakıldığında yerli firmalar ile aralarında çokta fark olmadığını görebiliyorsunuz.

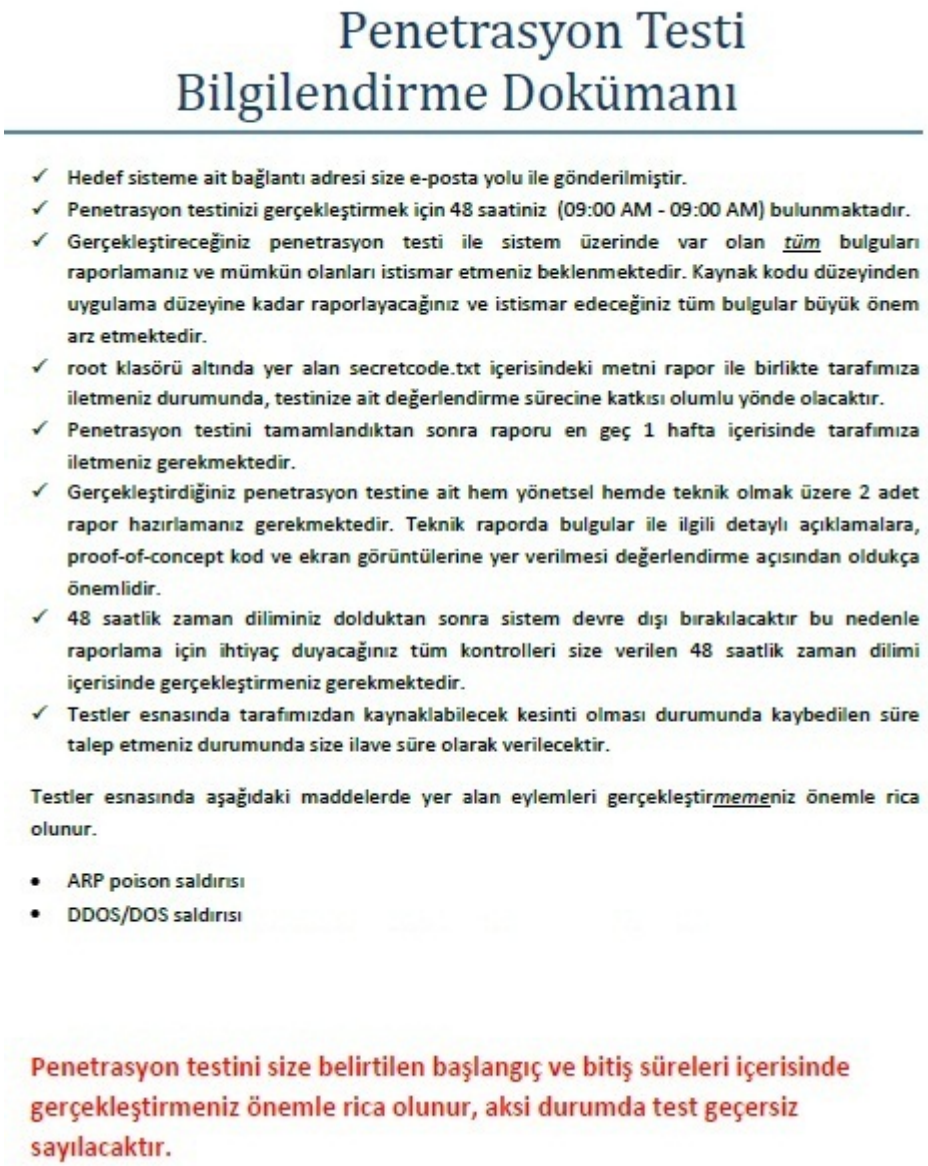
Honeypot hazırlama kısmına gelecek olursak internette bunun için fazla sayıda kaynak bulunuyor. Google'da ufak bir araştırma yaptığınızda CTF (capture the flag) için hazırlanmış bir çok sanal makina imajı ile karşılaşabilirsiniz. Bir tanesini alarak ihtiyaçlarınız doğrultusunda değiştirerek güzel bir değerlendirme tahtası oluşturabilirsiniz. Bende aynen bu şekilde bir imaj buldum ve üzerini özenle seçilmiş güvenlik zafiyetleri ile tamamladım.

Honeypot'un testi gerçekleştiren firmalar tarafından ele geçirilmesi için kafamda oluşturduğum yol, öncelikle web uygulamasının hack edilmesi, sistem üzerinde uzaktan komut çalıştırılarak sisteme netcat ve benzeri araçlar ile bağlantı kurulması ve daha sonra sistem üzerinde SUID bit'ine sahip olan ve üzerinde format string ve buffer overflow güvenlik zafiyeti bulunan uygulamanın istismar edilerek sunucunun ele geçirilmesi olmuştu. Buffer overflow ve Format String güvenlik zafiyetlerinin istismar edilebilmesi için sistem üzerindeki ön tanımlı korumaları kapatmayıda (Execshield, ASLR vs.) ihmal etmedim.

Öncelikle Honeypot'un işletim sisteminin (Fedora) yama seviyesini local istismar araçları ile istismar edilemeyecek seviyeye getirdim. Sanal makina imajının içerisinde md5 ile hashlenmiş yönetici şifresinin dışarıdan görüntülenmesine olanak sağlayan güvenlik zafiyetine sahip NanoCMS web uygulaması ve bunun dışında bir de eski sürüm Drupal portal bulunuyordu. NanoCMS, Drupal ve sistem üzerinde kurulu olan Mysql şifrelerini test1234, deneme1234 ve 1q2w3e4r gibi oldukça zayıf seçmeye özen gösterdim. Bunun dışında internetten C programlama dili ile kodlanmış bir echoserv daemonu buldum (echoserv dediğimiz servise telnet çektiğinizde ne girdi gönderirseniz çıktı olarak onu alıyorsunuz) ve FreeBSD telnet sunucusu gibi kendisini 65530. portta sunmasını sağladım. Sadece bununla kalmayarak sprintf() gibi tehlikeli fonksiyonlar kullanarak format string ve buffer overflow güvenlik zafiyetlerini itinayla oluşturdum :)

Kısaca en kolay yoldan sunucuyu ele geçirmek için izlenecek yol NanoCMS yönetici şifresinin hash hali alınacak, herhangi bir md5 çözücü ile çözülecek, NanoCMS yönetici paneline uzaktan komut çalıştırmaya imkan tanıyacak php kodu eklenecek ve daha sonrasında apache yetkisi ile uzaktan komut çalıştırılabilecekti. Daha sonra netstat çıktısı ve crontab dosyası incelenerek sistemde echoserv uygulamasının hangi portta hangi klasörde hangi yetki ile çalıştığı tespit edilecek ve istismar edilerek root yetkisi alınabilecekti.

Hazırlıklarımı tamamladıktan sonra her firmaya 48 saat süre vererek penetrasyon testlerini gerçekleştirmelerini ve tespit ettikleri güvenlik zafiyetlerini içeren hem teknik hem yönetsel raporu en geç bir hafta içerisinde göndermelerini talep ettim.



Penetrasyon Testi
Bilgilendirme Dokümanı

- ✓ Hedef sisteme ait bağlantı adresi size e-posta yolu ile gönderilmiştir.
- ✓ Penetrasyon testinizi gerçekleştirmek için 48 saatiniz (09:00 AM - 09:00 AM) bulunmaktadır.
- ✓ Gerçekleştireceğiniz penetrasyon testi ile sistem üzerinde var olan *tüm* bulguları raporlamanız ve mümkün olanları istismar etmeniz beklenmektedir. Kaynak kodu düzeyinden uygulama düzeyine kadar raporlayacağınız ve istismar edeceğiniz tüm bulgular büyük önem arz etmektedir.
- ✓ root klasörü altında yer alan secretcode.txt içerisindeki metni rapor ile birlikte tarafımıza iletmeniz durumunda, testinize ait değerlendirme sürecine katkısı olumlu yönde olacaktır.
- ✓ Penetrasyon testini tamamlandıktan sonra raporu en geç 1 hafta içerisinde tarafımıza iletmeniz gerekmektedir.
- ✓ Gerçekleştirdiğiniz penetrasyon testine ait hem yönetsel hemde teknik olmak üzere 2 adet rapor hazırlamanız gerekmektedir. Teknik raporda bulgular ile ilgili detaylı açıklamalara, proof-of-concept kod ve ekran görüntülerine yer verilmesi değerlendirme açısından oldukça önemlidir.
- ✓ 48 saatlik zaman diliminiz dolduktan sonra sistem devre dışı bırakılacaktır bu nedenle raporlama için ihtiyaç duyacağınız tüm kontrolleri size verilen 48 saatlik zaman dilimi içerisinde gerçekleştirmeniz gerekmektedir.
- ✓ Testler esnasında tarafımızdan kaynaklabilecek kesinti olması durumunda kaybedilen süre talep etmeniz durumunda size ilave süre olarak verilecektir.

Testler esnasında aşağıdaki maddelerde yer alan eylemleri gerçekleştir*meme*niz önemle rica olunur.

- ARP poison saldırısı
- DDOS/DOS saldırısı

Penetrasyon testini size belirtilen başlangıç ve bitiş süreleri içerisinde gerçekleştirmeniz önemle rica olunur, aksi durumda test geçersiz sayılacaktır.

Raporları incelediğimde yerli firmalardan bir tanesinin diğerlerinden daha iyi olduğu, diğer ikisinin aynı seviyede olduğu, bir tanesinin ise yeterli seviyede olmadığı ortaya çıktı. Beni asıl şaşırtan ise yabancı firmanın yerli firmalar kadar başarılı olamasmaıydı sebebi ise Honeypot üzerinde hem ağ hem web uygulamasına yönelik penetrasyon testi gerçekleştirmelerini talep etmemize rağmen sadece web uygulama penetrasyon testi gerçekleştirmiş olmalarıydı.

Tüm firmalar testlerini gerçekleştirdikten sonra kendilerini değerlendirebilmeleri için daha önce hazırlamış olduğum ufak cevap anahtarını kendileri ile paylaştım.

Sonuç olarak yazının başında da belirttiğim gibi firmaların hizmetlerine dair sizle paylaştıkları örnek raporlar, referanslar kağıt üzerinde dört dörtlük olabilir ancak hazırlamış olduğunuz honeypot üzerinde gerçekleştirecekleri ve size sunacakları rapor sizin için paha biçilmez olabilir…

CEH mi yoksa OSCP mi ?

written by Mert SARICA | 11 May 2012
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.