

Keşif

written by Mert SARICA | 14 March 2010

Ethical hacking hakkında bilgi sahibi olanlarınız bilirler, ethical hacking temel olarak 5 adımdan oluşur;

- Keşif (Reconnaissance)
- Tarama (Scanning)
- Erişim sağlama (Gaining access)
- Erişim koruma (Maintaining access)
- İzeri silme (Clearing tracks)

Kimilerine göre en önemli adım erişim kazanma adımı gibi görülsede aslında içlerinden en önemlisi keşiftir çünkü ethical hackingde asıl amaç saldırı tespit/önleme sistemlerine yakalanmadan, alarm mekanizmalarını devreye sokmadan hedef sisteme erişim sağlamak ve erişimi korumaktır. Hiçbir aklıselim kişinin hedef sistem ile ilgili keşfe çıkmadan önce direk hedefe metasploit db_autopwn (tüm istismar araçlarını hedefe yönlendirir) ile saldırmayacağı düşünülüğünde de keşif adımının önemi ortaya çıkmış oluyor.

Keşif adımı iki alt adımdan oluşur, pasif ve aktif.

- Aktif keşifte hedef sistem ile iletişim kurarak bilgi toplamaya çalışılır. (Örnek: ping)
- Pasif keşifte ise hedef sistem ile iletişim kurmadan bilgi toplamaya çalışılır. (Örnek: arama motorları)

Artık sunucularda kullanılan uygulamaların istismar edilme oranının geçtiğimiz senelere kıyasla daha düşük olması ve istemciler üzerinden gerçekleştirilen saldırıların sunuculara kıyasla daha yüksek etkiye sahip olması (heleki istemcinin masaüstünde diğer sunuculara ait şifreler bir dokümanda şifresiz olarak tutuluyor ise) istemci tarafındaki uygulamaları istismar etmeye yönelik saldırıları arttırıyor. Hatırlarsanız geçtiğimiz aylarda Google, Adobe ve bazı büyük firmalar Aurora (Internet explorer sıfır gün (0 day) saldırısı) saldırısına maruz kalmışlardı.

Bu durumda kurum olarak izlenmesi gereken politikaların başında kurum içerisinde kullanılan yazılımların (özellikle ips, antivirüs) dışarıya sızdırılmaması geliyor. Örneğin kurumunuza gerçekleştirilecek hedeflenmiş bir saldırı hazırlığında olan kötü niyetli bir kişinin amacı ilgili kişinin e-

posta adresine trojan göndermek ise yapacağı ilk iş antivirüse yakalanmamasını sağlamak olacaktır. 20 farklı antivirüs motoru ile uğraşmak yerine kurumunuzda kullanılan antivirüs yazılımını hangisi olduğunu biliyor ise bu yazılıma odaklanacaktır.

Hedeflenmiş bir saldırıya maruz kalma ihtimalinin düşük olduğunu düşünsenizde yerli hacking forumlarına göz attığınızda yüzlerce kişinin trojanların, keyloggerların antivirüs yazılımlarına yakalanmamaları adına hummalı çalışmalara devam ettiğini ve bu trojanların ve keyloggerların 300-1000 TL arasında alıcı bulunduğunu görebilirsiniz.

Kısa bir bilgilendirmeden sonra neden bu yazıyı yazdığımı gelebiliriz. Geçtiğimiz günlerde bir iş ilanı örneğine ihtiyacım vardı ve iş ilanı sitelerinde CISSP anahtar kelimesi ile aramalar yapıyordum. Bir arama sonucunda bir firmanın iş ilanında kullandığı antivirüs yazılımından IPS teknolojisine kadar gizlenmesi gereken tüm bilgileri paylaştığını gördüm.

The screenshot shows a job advertisement on the CVPlus website. The ad is for a 'Bilgi Ağı Ve Güvenliği Uzmanı' (Network and Security Specialist) position. The job description includes requirements for CISSP, CISO, and various security technologies like IPS, IDS, and SIEM. The ad is dated 09.03.2010 and is for a position in Istanbul, Avrupa.

Bilgi Ağı Ve Güvenliği Uzmanı

Bugün
İstanbul Avrupa

İlan Tarihi : 09.03.2010
Sektör :
İ : İstanbul Avrupa
Alınacak Personel Sayısı : 1

İşin Tanımı :

in ihtiyaç duyduğu veri iletişim altyapısı ve bu altyapının güvenlik ihtiyaçlarının analizi, gerekli kontroller ve önlemler ile sorumlu olduğu sistemleri en verimli şekilde çalıştırılmasını sağlanması.

Aranan Nitelikler :

- Üniversitelerin Bilgisayar, Elektronik Haberleşme Mühendisliği veya ilgili bölümlerinden mezun
- En az 2 yıl Bilgi Teknolojileri Ağ ve Güvenlik konusunda deneyimli TCP/IP , routing, switching konusunda deneyimli
- Firewall(Checkpoint, PIX vb) ürünleri hakkında deneyimli Raporlama ve log inceleme deneyimine sahip
- Url Filtering (Websense) IPS teknolojileri (IBM ISS) ve Trend Micro Antivirüs ürünleri hakkında bilgi sahibi
- Terchen CISSP, CISO eğitimlerini almış veya bilgi sahibi Linux,
- Windows işletim sistemleri konusunda bilgi sahibi
- İyi derecede İngilizce bilgisine sahip
- Ehliyet sahibi ve seyahate engeli olmayan
- Ekip çalışmasına yatkın, proaktif ve sonuç odaklı çalışan
- Erkek adaylar için askerlik hizmetini tamamlamış

Hemen aklıma Çinli general Sun Tzu'nun söylediği o meşhur söz aklıma geldi

To know your Enemy, you must become your Enemy

Bu sözden yola çıkarak acaba ufak bir program yardımı ile anahtar kelimeler ile firmaları eşleştirerek firmalar hakkında ne kadar bilgi edinebilirim sorusuna yanıt aramaya karar verdim ve bilgi edinmek için örnek olarak SecretCV ilan sitesini kullanan bir program hazırladım.

```
C:\Windows\system32\cmd.exe

=====
İlan Arama Uygulaması v1.0
=====
[+] Anahtar kelime: trend micro

[+] Anahtar kelime ile ilişkili firmalar:

[*] Firma: ██████████
[**] İlan: http://www.secretcv.com/ilan/████████████████████████████████████████
[**] İlanda tespit edilen potansiyel üretici/yazılım bilgileri:
    Windows
    Iss

[*] Firma: ██████████

[*] Firma: ██████████
[**] İlan: http://www.secretcv.com/ilan/████████████████████████████████████████
1
[**] İlanda tespit edilen potansiyel üretici/yazılım bilgileri:
    Pix
    Iss
    Checkpoint
    Windows
    Trend micro
    Websense

[*] Firma: ██████████

-----
http://www.mertsarica.com

C:\Users\Mert\Desktop>
```

Ben yapıyorsam düşmanım daha da iyisini yapardan yola çıkarsak firmaların kullandığı yazılımları ilan siteleri üzerinden tespit etmenin kolay olduğunu bunun dışında firmaların kurum içerisinde kalması gereken yazılım/üretici bilgilerini farkındalık eksikliği nedeniyle ilanlara taşıdıklarını görebiliyoruz. Özetle verdiğimiz iş ilanlarına, yazışmalara dikkat edelim diyerek bu haftaki yazıma burada son veriyorum.

POC programı buradan temin edebilirsiniz.