ÖN BİLGİ

Bu belgenin resmi adresi bulunamamıştır. Alternatif adreste yedeklenmiştir. Bu belge

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Kendimi%20Nas%C4%B1l%20Yeti%C5%9Ftirebilirim.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Bilisim sektörü diğer sektörlere göre hem biraz kolay hem de biraz zordur. Kolaylığı her eline bilgisayar geçirenin bu sektörde kendini geliştirebileceği . Zor yönü ise –ki bence unutulan yönülüdür- bilgisayarında bir bilim dalı olduğu ve üzerinde özenli çalışma gerektirdiğidir.

(Page 1)

2)

Herhangi bir konuda yetkin kişiliğe sahip olmak istiyorsanız öncelikle bir tercihde bulunmanız gerekiyor. Sektör “Hüzeyfe”nin bakış açısına göre temel olarak 4 birime ayrılmaktadır:

- Yazılım
- Ag ve Guvenlik
- Sistem Yoneticiligi
- Veritabani Yoneticiligi

Bunların dışında da birçok birim vardır fakat benim ilgi alanım ve piyasanın en fazla istek duyduğu alanlar bunlar olduğu için bu yazıda bu kadarına değinilecektir.

(Page 1)

3)

Network konusunda ilk öğrenilesi protokoller ARP, ICMP, IP, UDP ve TCP’dir. Bu protokollerin yapılarını okuduğunuz kitaptan öğrendikten sonra trafik analiz programları ile protokol başlık bilgilerini anlamaya çalışın. Hemen hemen diğer tüm protokoller bu 4 ana protokol üzerine kuruludur. Bir nevi internetin temeli bu 4’lüdür diyebiliriz.

Kendi kendinize normal olmayan TCP, UDP, icmp ve arp paketleri oluşturarak bunlara karşı işletim sistemlerinin ya da güvenlik duvarlarının nasıl tepkiler verdiğini paket analiz programları kullanarak analiz etmeye çalışın.

(Page 4)

4)

Network-Güvenlik eğitimlerinde Hüzeyfe Önal'ın temel olarak kullandığı bazı çalışma yöntemleri şunlardır:

Senaryo 1

Araçlar: Wireshark, tcpdump, snoop

Aksiyon: Bulunduğunuz ağda 30 saniyeliğine tcpdump ya da Wireshark çalıştırarak yeteri kadar paket kaydedin. Ardından kaydedilen bu paketlere bakarak gelen-giden paketlerin Katman2, Katman 3, Katman 4'te (OSI katmanlarında) hangi protokolleri kullandığını tespit edin. Katman 2 için ne tür arp mesajları var gibi, arp başlık bilgilerini neler gibi sorulara cevap arayın.

Sonuç: Bu senaryo ile paket sniffer'larının nasıl çalıştığını, ayrıca ham trafikten protokol türünün nasıl tespit edildiğini öğrenmiş olacaksınız.

Senaryo 2

Araçlar: Nmap, Pakit // Bence hping3 de olmalı(!).

Aksiyon: Araçlardan herhangi birisini kullanarak kaynak IP'si ve hedef IP'si aynı olan, aynı zamanda kaynak portu ve hedef portu aynı olan TCP ve UDP paketleri oluşturarak bu paketleri Wireshark veya tcdump ile dinlemeye alın. İşletim sistemi böyle bir paket aldığında nasıl davranıyor gözlemleyin.

Ayrıca paket oluşturma araçlarından biriyle sahte arp paketleri göndererek internet iletişimini bozmaya çalışın. Örneğin aynı ağdaki bir makineye gerekli ICMP paketlerini göndererek kurbanın sizi default gateway sanmasını sağlayın.

Sonuç: Bu senaryo ile yukarıda verilmiş paket oluşturucu araçları kullanarak istenilen özellikte sahte TCP, UDP, ICMP ve ARP paketleri oluşturma deneyimine vakıf olmuş olacaksınız ve ayrıca bu oluşturulan paketlerin başlıklarını detaylı bir şekilde öğrenmiş olacaksınız.

Senaryo 3

Araçlar: nslookup, dig, UrlSnarf, ParosProxy, samspade vs...

Aksiyon: Bir DNS sorgusunun nasıl gitgellere uğradığını öğrenmek için bir sniffer programını kendi makinanızın UDP Port 53'ünü dinleyecek şekilde yapılandırın. Ardından aynı makine ile nslookup programını kullanarak bir web sitesinin IP'sini edinmeye çalışın. Bu süreç sırasında sniffer'ınızın yakaladığı DNS paketlerini incelemeye alın.

Makineninizi web sitelerine bağlandığınız zaman göndereceğiniz HTTP Request'leri yakalayabilecek şekilde yapılandırın. Bunun için ParosProxy ya da urlSnarf programlarını kullanın. Bir siteye girdiğinizde kaç HTTP Request paketinin gittiğini ve bunlardan kaçının orijinal siteye ait olduğunu not edin. Ardından içinde resim ya da harici bir link taşımayan statik bir sayfaya bağlanın ve bir önceki yakalanan paketlerle şimdikinin farkını kıyaslayın.

HTTP Header bilgileri hakkında ve cookie'lerin nasıl çalıştığı konusunda bilgi sahibi olmaya çalışın. Bu parametrelerle oynayarak neler yapılabileceğini öğrenmeye çalışın. (Örn; Bir kurbanın cookie bilgisini elde eden saldırgan kendi makinesinin cookie header'ına kurbanınkini yerleştirerek kurbanın oturumunu devralabilir. | Bu örnek benim notumdur. Çerezi biliyorum, fakat http header parametreleriyle oynanarak neler yapılabileceğini bilmiyorum.).

Senaryo 4

Araçlar: Iptables, OpenBSD veya FreeBSD Packet Filter'ı (PF'i), Nmap, Tcpdump

Aksiyon: Üzerinde SSH ya da Telnet çalıştıran hedef bir Linux ya da BSD sisteme ssh/telnet ile bağlanmaya çalışın. Bu bağlantı boyunca gönderdiğiniz paketleri hedef linux sisteminin dinlemesi için hedef sistemde bir tool kullanın. Bu tool ilgili porttan gelen paketleri bir köşeye not etsin. Daha sonra hedef linux'un güvenlik duvarını kullanarak ssh/telnet bağlantısı için gelen istekleri sınırlandırın (ilgili hedef sistemin portunu sınırlandırın) ve tekrar hedef linux'a bağlanmaya çalışın. Bu sırada yine trafiği hedef linux kaydetsin ve bir önceki durum ile sonraki trafiği karşılaştırarak güvenlik duvarı devreye girmeden önce ve sonra ne gibi farkların meydana geldiğini gözlemleyin.

İkinci olarak hedef linux sistemdeki güvenlik duvarı aracılığıyla hedef sisteme gelen ICMP Echo Request paketlerini, yani ping paketlerini engelleyin. Bunun akabinde nmap ile hedef linux'a ping atma methodunu kullanarak nmap taraması yapın ve sonuçlarını kaydedin. Ardından Nmap'i karşı sisteme ICMP Echo Request göndermeyecek şekilde tarama yapması konusunda yapılandırın (uygun parametrelerini kullanın) ve hedef linux sistemine yapılan tarama işlemini bu yeni perspektifle tekrarlayın. Böylece bir önceki tarama ile sonraki taramayı karşılaştırarak ping paketlerine karşı set çekmenin nmap'i nasıl etkilediğini tespit edin.

(page 5-6)

5)

El Altında Bulundurulması Gereken Programlar

i) Tcpdump
- Akan trafiği gözlemlemek ve incelemek için kullanışlı bir araçtır.

ii) IpTables ve Packet Filter For BSD Systems
- Güvenlik duvarlarının (Firewall'ların) paketleri nasıl yönettiğine dair bilgiler edinebileceğiniz araçlardır.

(Page 7)