Cybook Orizon Mini Pentest

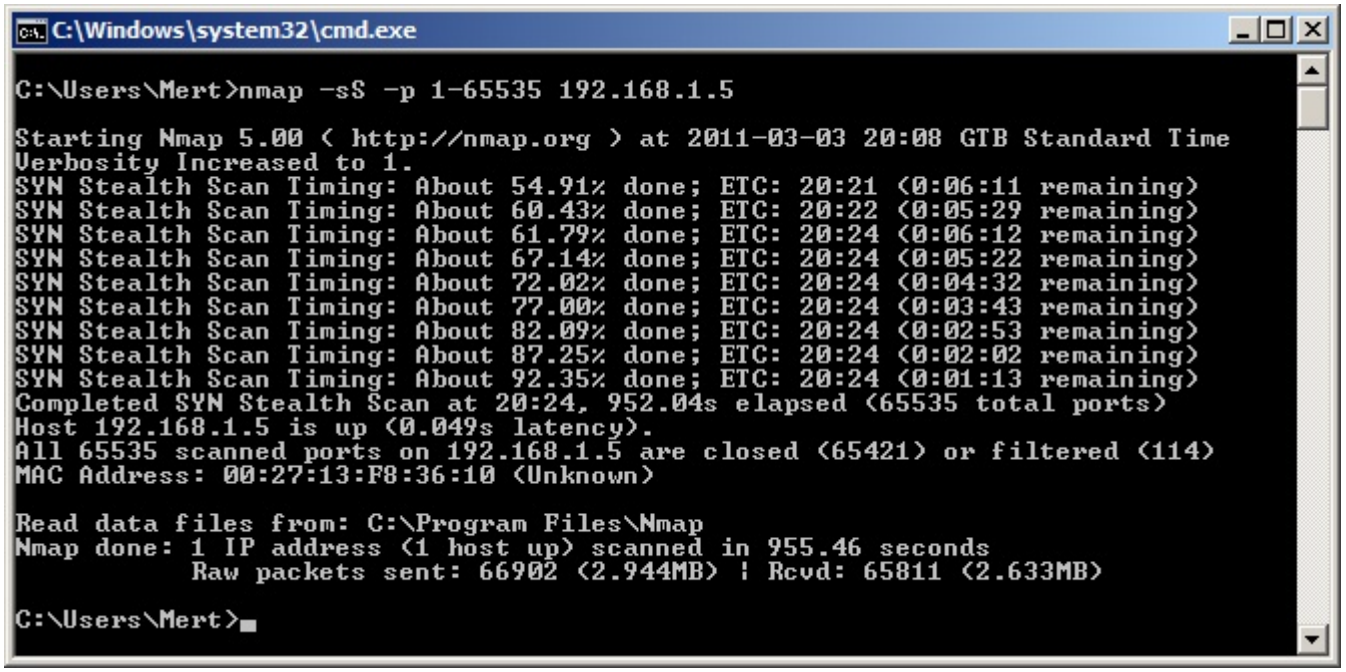
written by Mert SARICA | 19 April 2011

Bilişim güvenliği ile ilgili teknik kitaplar okumaya bayılıyorum özellikle beni zorlayan, çıta yükselten kitaplar oldu mu tadından yenmiyor. Kitap okumadığım zaman geri kaldığımı düşünerek kendimi kötü hissediyorum bu nedenle kitap okuma konusunda ilginç bir motivasyona (takıntı da denebilir :)) sahibim. Üniversite zamanında hayatımın büyük bir bölümü bilgisayar başında e-book okumak ile geçerken iş hayatına geçiş sonrasında e-book çıktıları ile gezer durur oldum. Özellikle işe giderken ve işten gelirken serviste kitap okumak benim için büyük bir keyif ancak her gün 10-20 sayfalık çıktı almak, A4'e bassan kocaman, kitapçık yapsan küçücük, kağıt israfı, göz yorgunluğuydu derken okuma aşkı beraberinde bir çok sorunu da getiriyor.

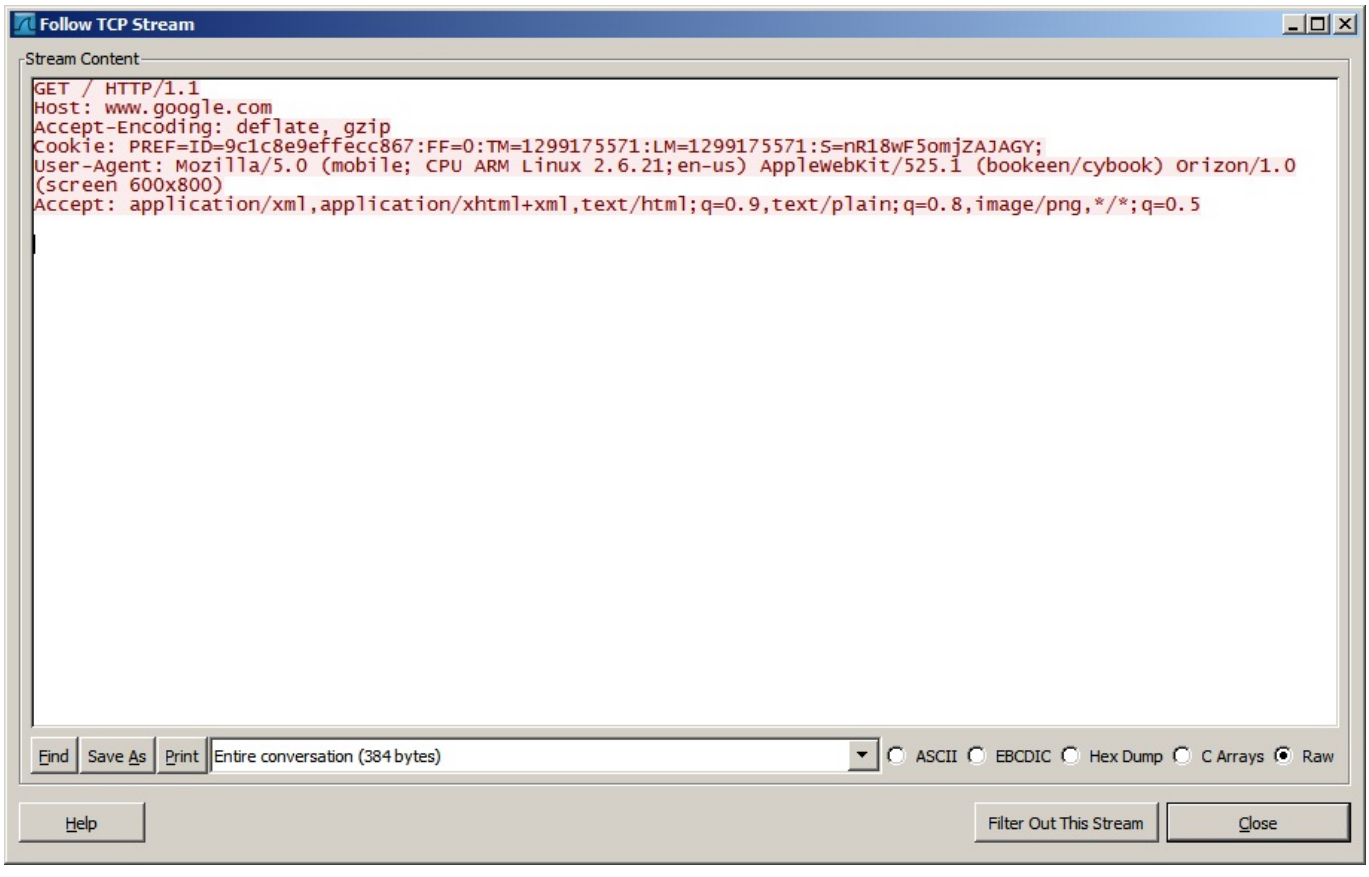
Neyse ki nişanlım duruma müdahale ederek geçtiğimiz aylarda bana bir e-book okuma cihazı hediye etti, Cybook Orizon. Dünyanın en ince e-book okuma cihazı olmasının yanısıra hafif olması (250 gr), dokunmatik ekrana sahip olması, micro-usb girişinin olması, 2 GB dahili belleğe, WIFI, bluetooth ve akselerometreye (accelerometer) sahip olması beni memnun eden özelliklerinin başında geliyor.

Ahlaklı korsana hediye edilen elektronik cihazın ufak çaplı penetrasyon testinden geçirilmemesi gibi bir durum söz konusu olamazdı, olmadı da :)

Teste ilk olarak port taraması ile başladım ve hiç açık port bulamadım.



Daha sonra ARP zehirleme ile MITM (ortadaki adam) saldırısı gerçekleştirerek tüm trafiği izlemeye başladım. Web trafiğinden elde ettiğim bilgiler sayesinde cihaz üzerinde ARM Linux kullanıldığını, 2.6.21 kernel sürümüne sahip olduğunu ve Mozilla tabanlı özelleştirilmiş bir internet tarayıcısı kullanıldığını öğrendim.



Internet tarayıcısında denediğim about:config ve benzer yöntemlerin hiçbiri işe yaramadı. Bunun üzerine IKAT (Interactive Kiosk Attack Tool)'in sitesine

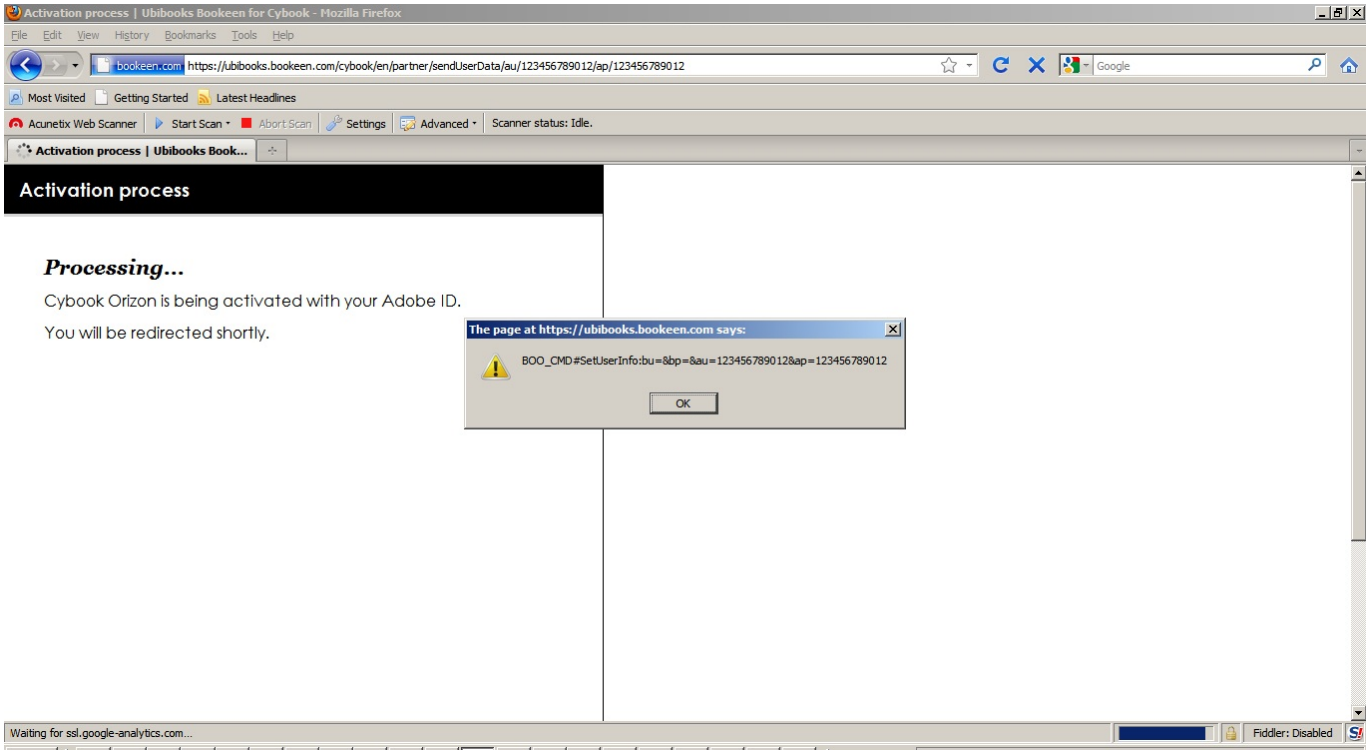
bağlanarak internet tarayıcısı üzerinden işletim sistemine erişecek yöntemleri de teker teker denedim ancak yine başarılı olamadım.

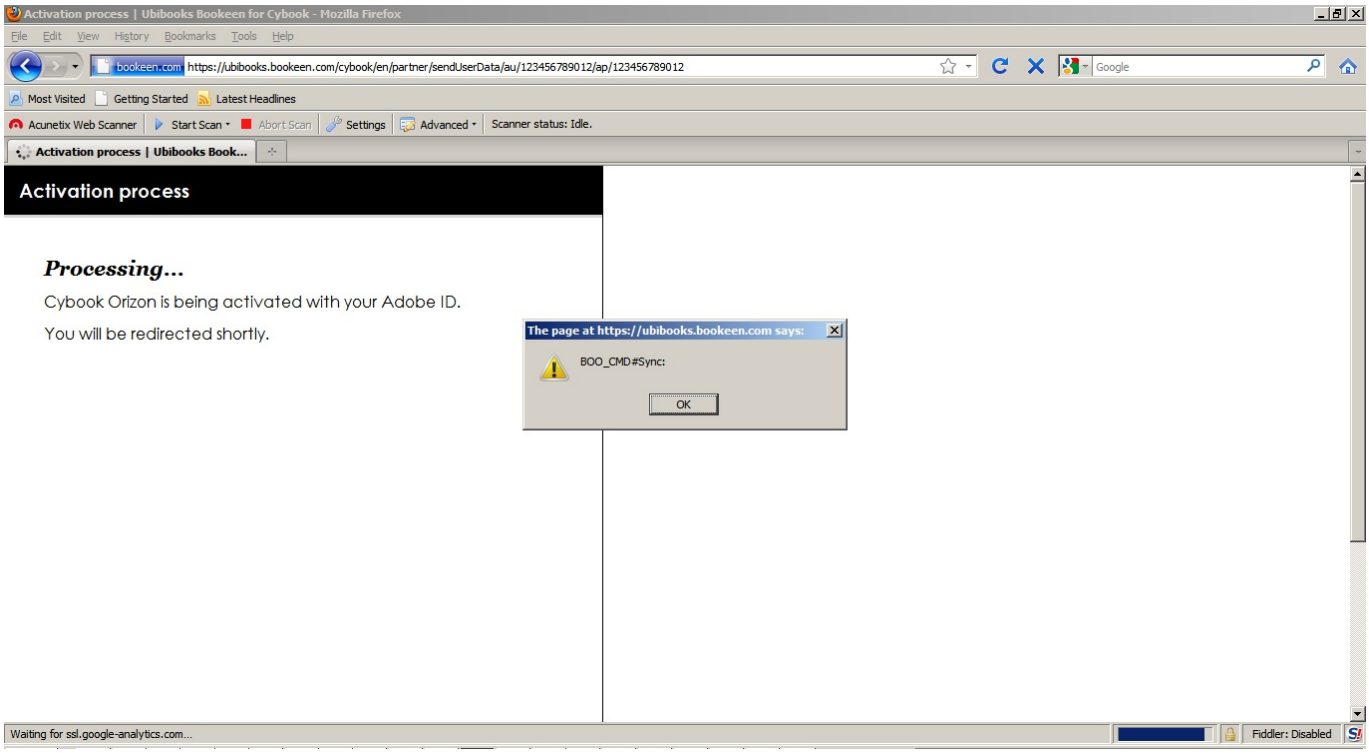
Cihaz üzerinde bluetooth desteği olduğunu söylense de henüz aktifleştirilmemiş ve yerleşik yazılım (firmware) güncellemesi ile aktifleştirileceği belirtiliyor. Bu durum aslında yerleşik yazılım üzerinde bir çok opsiyonun gizlendiğine işaret ediyor. Cybook'un sitesinden indirmiş olduğum yerleşik yazılımı incelediğimde normal olarak anlamlı hiçbir karakter dizisi ile karşılaşmadım. Karakter dağılımına baktığımda ise neden karşılaşmadığım ortadaydı. Yerleşik yazılım üzerinde yer alan ilk 5 bayt (Boo16) dikkatimi çekti ancak arama motorları üzerinde yaptığım araştırmalar sonuçsuz kaldı. Yerleşik yazılım üzerinde manipülasyonlar gerçekleştirerek ipuçları elde etme yolunu tercih etmek isterdim ancak yazılımın bozulması durumunda bana yol, köprü, baraj olarak geri döneceği için daha ileri gitmedim :)

Dec	Hex	Char	Count	Percent
11	0x0B		127135	0.39%
159	0x9F		127046	0.39%
44	0x2C	','	127026	0.39%
252	0xFC		126979	0.39%
139	0x8B		126975	0.39%
72	0x48	'H'	126958	0.39%
2	0x02		126958	0.39%
206	0xCE		126950	0.39%
238	0xEE		126931	0.39%
220	0xDC		126885	0.39%
131	0x83		126882	0.39%
216	0xD8		126881	0.39%
58	0x3A	':'	126881	0.39%
190	0xBE		126848	0.39%
96	0x60	'`'	126844	0.39%
192	0xC0		126823	0.39%
52	0x34	'4'	126790	0.39%
219	0xDB		126768	0.39%
128	0x80		126738	0.39%
81	0x51	'Q'	126729	0.39%
32	0x20	' '	126721	0.39%
88	0x58	'X'	126702	0.39%
157	0x9D		126698	0.39%
130	0x82		126690	0.39%
87	0x57	'W'	126690	0.39%
148	0x94		126688	0.39%
211	0xD3		126686	0.39%
240	0xF0		126683	0.39%

Cihaz üzerinde yer alan menülerde gezinirken Ebook Store menüsünün ilginç işlevi dikkatimi çekti. Bu menüye girince internet tarayıcısı otomatik olarak sizi Cybook'un bir alt sitesine yönlendiriyor ve cihazı ADOBE ID ile aktifleştirmenizi sağlıyor. Buraya kadar herşey normal ancak aktifleştirme kısmında javascript ile cihaza gönderilen komutlar dikkatimi çekti. BOO_CMD ile gönderilen her komutun bir işlevi bulunuyor ve site bağımsız olarak bu komutları nerede görürse görsün aynı işlevi yerine getiriyor. Komutları ortaya çıkartmak (enumerate) için ufak bir betik (script) hazırlayarak # karakterinden sonra gelebilecek en fazla 4 karakterden oluşan komutları (daha

fazlası web sayfasının boyutunu büyütüyordu) oluşturdum ve daha sonra cihazın oluşturduğu trafiği izlemeye başladım ancak Sync dışında trafik oluşturan herhangi bir komut karşılaşmadım.





Son olarak cihazın güvenli bir siteye (SSL) bağlanma esnasında sahte sertifika ile karşılaşması durumunda nasıl bir aksiyon aldığını görmek için ufak bir test gerçekleştirdiğimde beni üzen bir durum ile karşılaştım. Cihaz güvenli bağlantının kurulması esnasında MITM saldırısı gerçekleştirilmesi durumunda herhangi bir uyarı vermeden iletişim kurmaya devam ediyor yani

Starbucks’ta kahvenizi yudumlarken bir yandan e-postalarımı güvenli bir şekilde kontrol edeyim deme gibi bir şansınız ne yazıkki bulunmuyor.

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