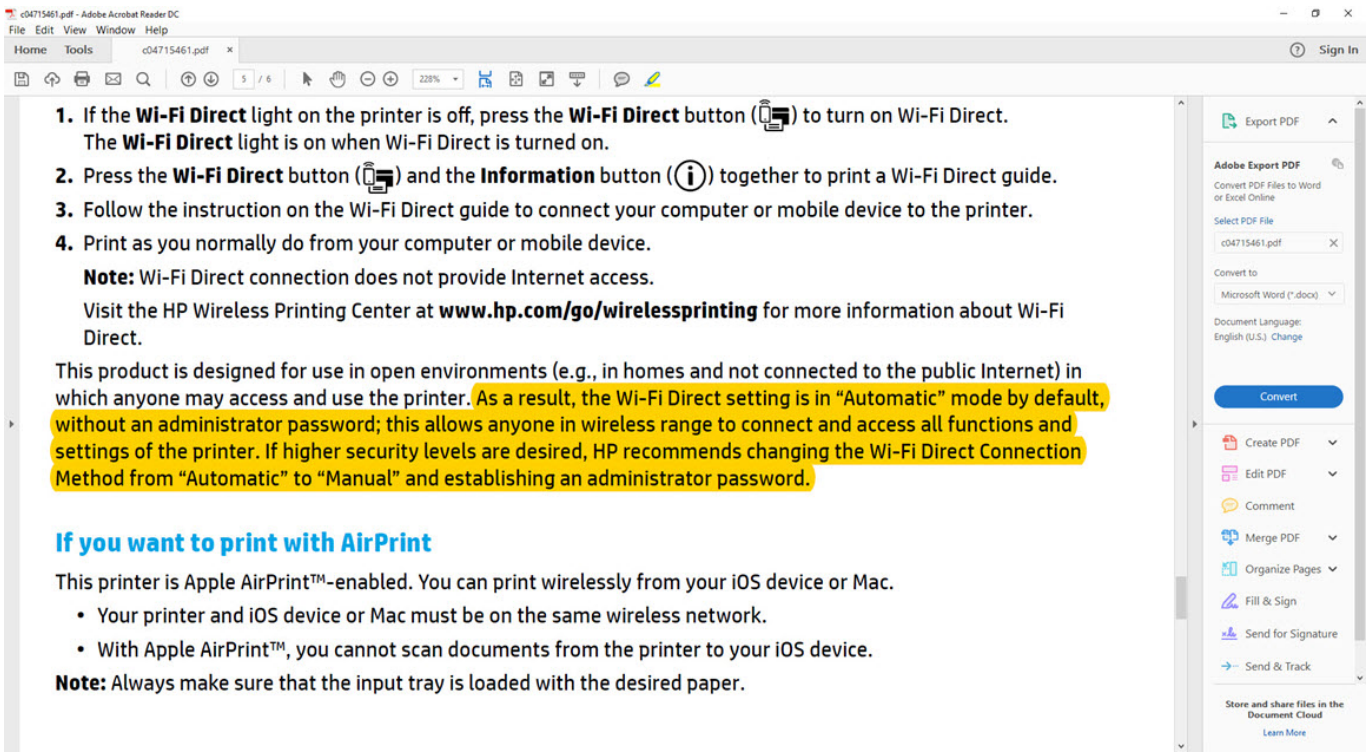
Yazıcı Deyip Geçmeyin!

written by Mert SARICA | 1 February 2018
If you are looking for an English version of this article, please visit here.

Aylar önce eşimin ihtiyaç duyması üzerine satın almak için bir yazıcı (printer) arayışı içine girdim. En son 15 yıl önce evinde yazıcı bulunduran biri olarak, e-ticaret sitelerini gezerken yazıcı fiyatlarının fiyat ve performans açısından geçtiğimiz yıllara oranla çok daha makul seviyelere gelmiş olması beni sevindirdi. “İnsanoğlu doyumsuzdur.” sözünün hakkını vererek, ucuz olsun, tarayıcısı da olsun, fotokopi de çekebilsin, Wi-Fi desteği de olsun, mobil cihazdan çıktı da rahatlıkla alınabilsin derken karşıma HP firmasının DeskJet 3630 All-in-One yazıcısı çıktı ve 200 TL’ye satın aldım.

Eşimin, “kurcalama, bozacaksın!” haklı isyanlarına aldırış etmeden, evimin yerel ağına dahil edeceğim bu yeni cihaza hızlıca göz atmaya karar verdim. HP Easy Start uygulaması sayesinde 5 dakika gibi bir sürede mevcut Wi-Fi ağımın

parolasını uygulamaya girerek yazıcıyı kablosuz ağıma kısa bir sürede dahil edip, kurulumu hızlıca tamamlayabildim. Kurulum adımlarında, güvenlik namına dikkat edilmesi gereken hususlara, güçlü yönetim arayüzü parolasının belirlenmesine dair herhangi bir yönlendirme göremedim. Halbuki bu yazıcı, Wi-Fi cihazların kendi aralarında veri alışverişi yapabilmesine de olanak sağlayan Wi-Fi Direct teknolojisine de sahipti. Yazıcının kurulum belgelerine baktığımda, yüksek güvenlik seviyesi için Wi-Fi ayarının otomatikten manuele değiştirilmesi gerektiği söylense de, nasıl yapılacağına dair kullanıcıya herhangi bir bilgi verilmiyordu.



1. If the **Wi-Fi Direct** light on the printer is off, press the **Wi-Fi Direct** button ( ) to turn on Wi-Fi Direct. The **Wi-Fi Direct** light is on when Wi-Fi Direct is turned on.
2. Press the **Wi-Fi Direct** button ( ) and the **Information** button ( ) together to print a Wi-Fi Direct guide.
3. Follow the instruction on the Wi-Fi Direct guide to connect your computer or mobile device to the printer.
4. Print as you normally do from your computer or mobile device.

   Note: Wi-Fi Direct connection does not provide Internet access.

   Visit the HP Wireless Printing Center at **www.hp.com/go/wirelessprinting** for more information about Wi-Fi Direct.

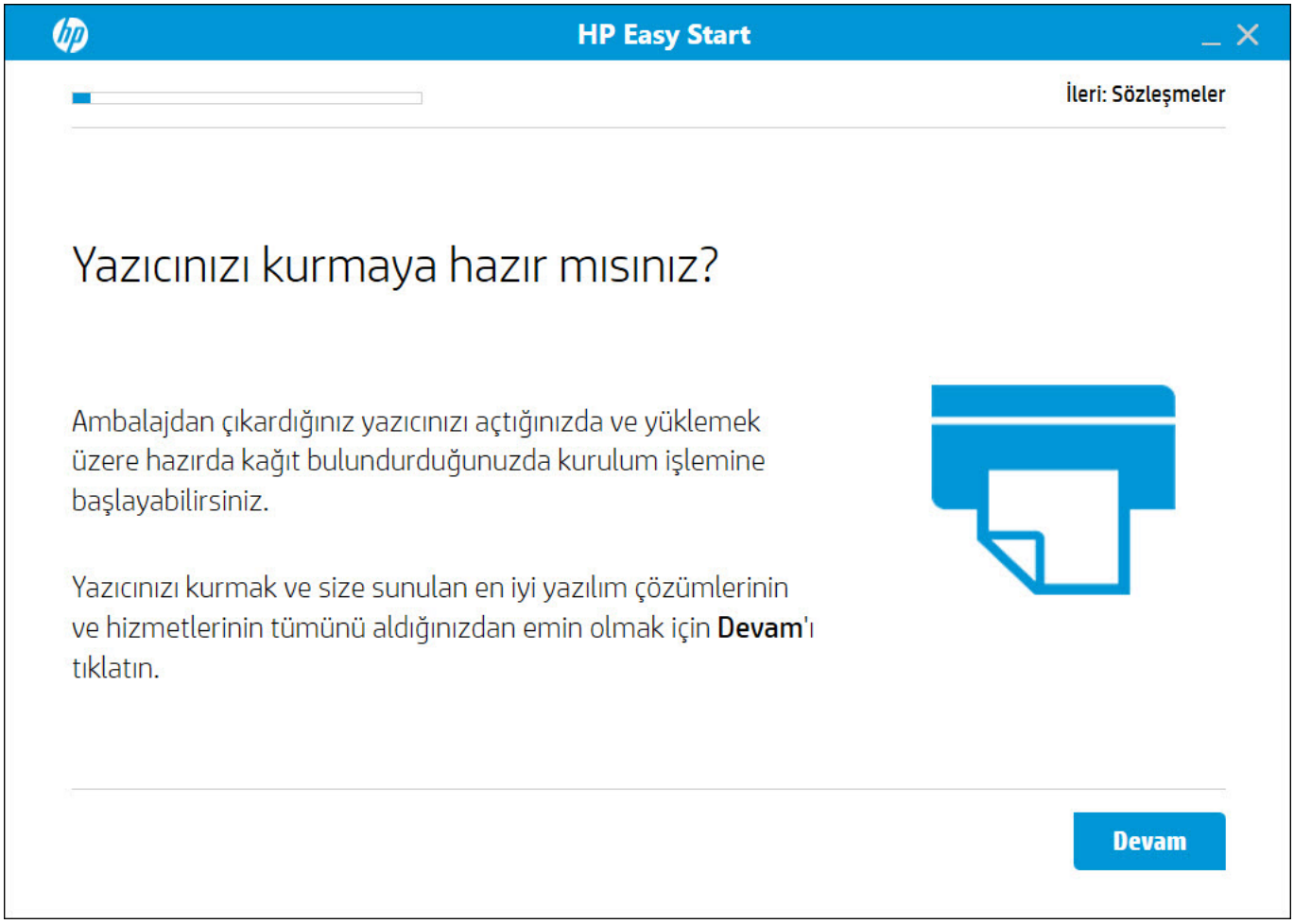
This product is designed for use in open environments (e.g., in homes and not connected to the public Internet) in which anyone may access and use the printer. As a result, the Wi-Fi Direct setting is in "Automatic" mode by default, without an administrator password; this allows anyone in wireless range to connect and access all functions and settings of the printer. If higher security levels are desired, HP recommends changing the Wi-Fi Direct Connection Method from "Automatic" to "Manual" and establishing an administrator password.

If you want to print with AirPrint

This printer is Apple AirPrint™-enabled. You can print wirelessly from your iOS device or Mac.

- Your printer and iOS device or Mac must be on the same wireless network.
- With Apple AirPrint™, you cannot scan documents from the printer to your iOS device.

Note: Always make sure that the input tray is loaded with the desired paper.



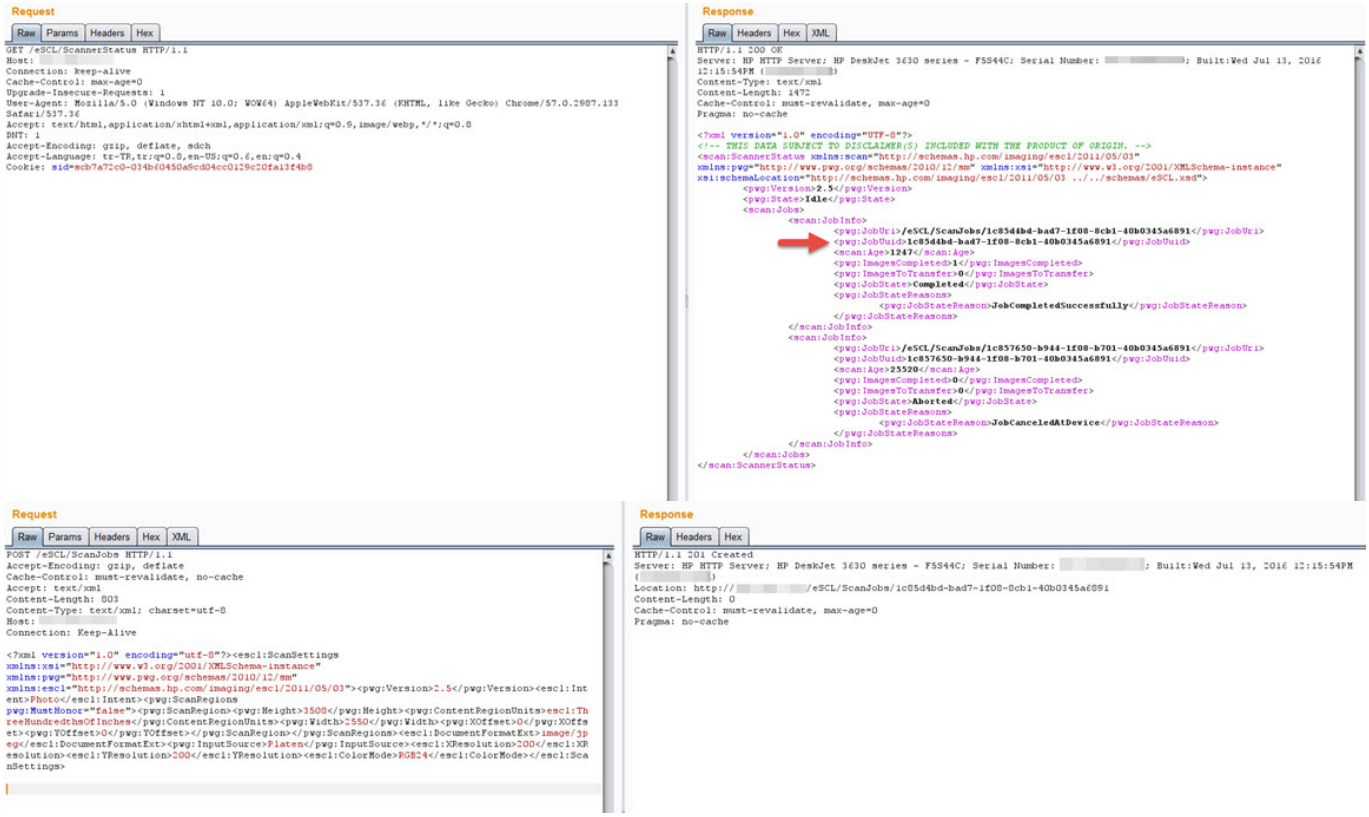
Yazıcı üzerindeki Wireless ve Information tuşlarına bastığımda Wi-Fi Direct parolasının 12345678 olduğunu öğrendim. İşin üzücü yanı ise bu kadar basit bir parolanın kurulum esnasında kullanıcı tarafından değiştirtilmesi çok zor olmasa gerekirdi. Malumunuz aldığı bir cihazı efendi gibi kullanmak yerine kurcalamayı tercih eden biri olarak aklıma takılan “Peki Wi-Fi Direct için varsayılan olarak kullanılan bu parola nasıl kötüye kullanılabilirdi ?” sorusuna yanıt aramaya başladım.

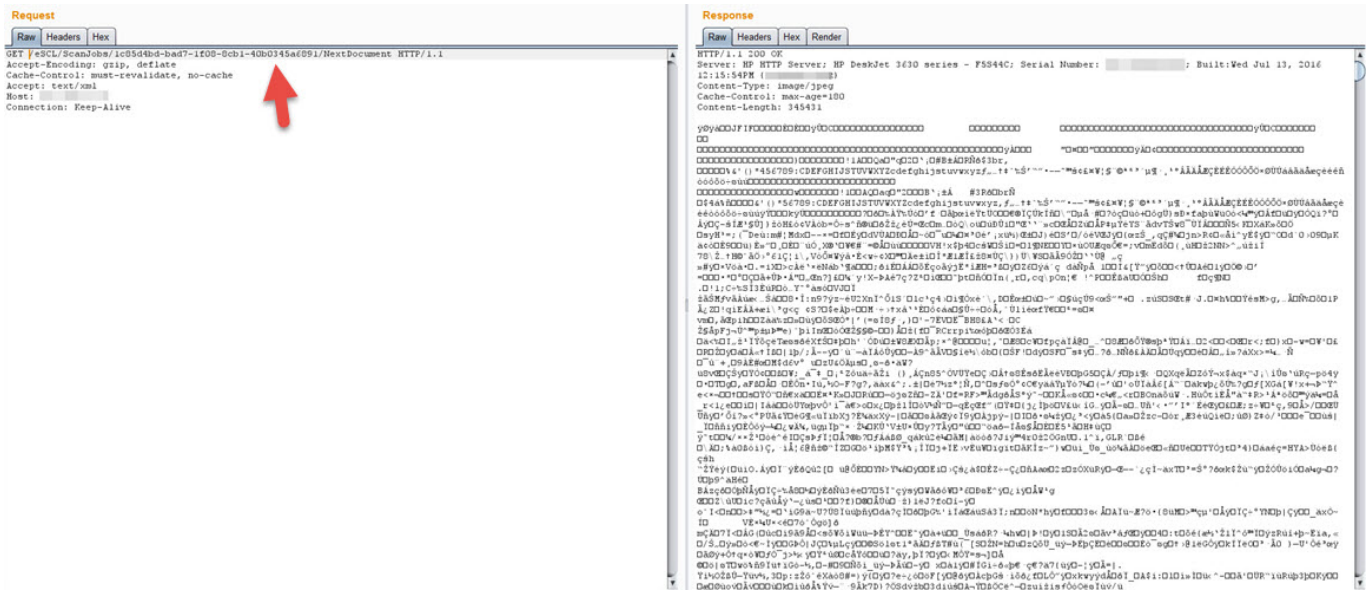
Zaman zaman nüfus kağıtlarıyla işlem yapılan abone merkezlerinden, noterlere kadar iş merkezlerinin ve iş hanlarının yoğun olduğu bölgelerde bu yazıcının ve tarayıcısının aktif olarak kullanıldığını bir hayal edelim. Yetkilinin görevlerinden biri de, işlem esnasında müşteriden aldığı nüfus kağıtlarını taratmak olsun. Peki art niyetli bir kişi yazıcıya Wi-Fi Direct üzerinden 12345678 parolası ile bağlanıp, hali hazırda başarıyla tamamlanmış bir tarama işlemine ait görüntü dosyasını yazıcıdan indirebilir mi ? Bu sorunun yanıtı ne mutlu ki hayır çünkü yazıcı, indirilen görüntü dosyasının 2. defa indirilmesine izin vermiyor ve muhtemelen de belleğinden siliyor.

Peki bu art niyetli kişi, yazıcının durumunu web servis üzerinden takip etse ve bir tarama işlemi başladıktan, tamamlandıktan hemen sonra 1 tarama işlemi

de kendi başlatsa ve görüntü dosyasını indirse kimin ruhu duyar ? Hele bir de bunu Python ile kodladığı bir araç ile Raspberry Pi üzerinde çalıştırırsa işin renginin ne denli değişeceğini az çok tahmin edebiliriz. Raspberry Pi tarafı ile ilgili bir çalışma yapmasam da Python ile HP Scanner Thief adında ufak bir araç geliştirip bunu kötüye kullanmanın pratikte ne kadar kolay olabileceğini gösterme ve farkındalık yaratma adına hızlıca bir çalışma yapmaya karar verdim.

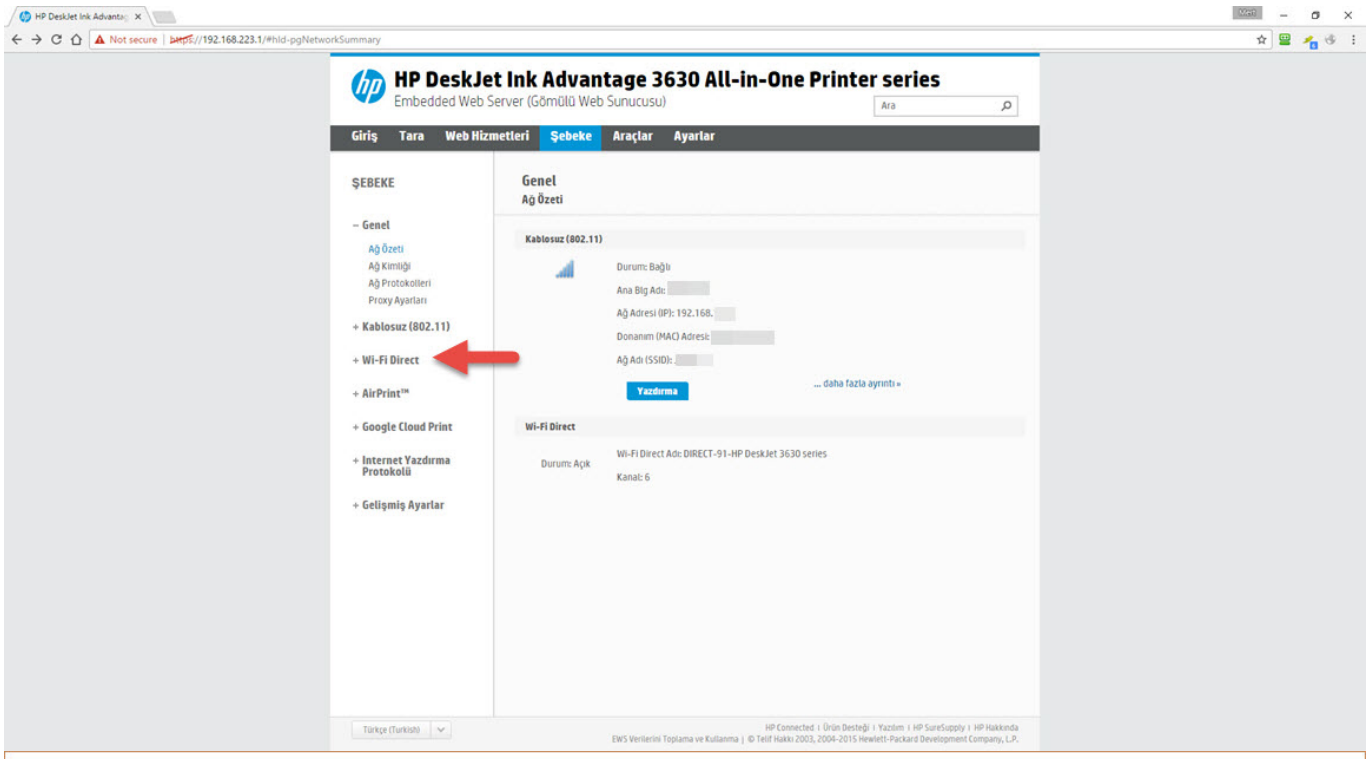
HP Scanner Thief aracının temel olarak yaptığı, tarayıcının durumunu kontrol etmek için /eSCL/ScannerStatus sayfasına istekte bulunmak ve JobUuid değeri daha önceki değerden farklı ise /eSCL/ScanJobs sayfasına tarama işlemini başlatma isteği göndermek ve ardından oluşan dokümanı /eSCL/ScanJobs/[uuid]/NextDocument sayfasından indirmekti.

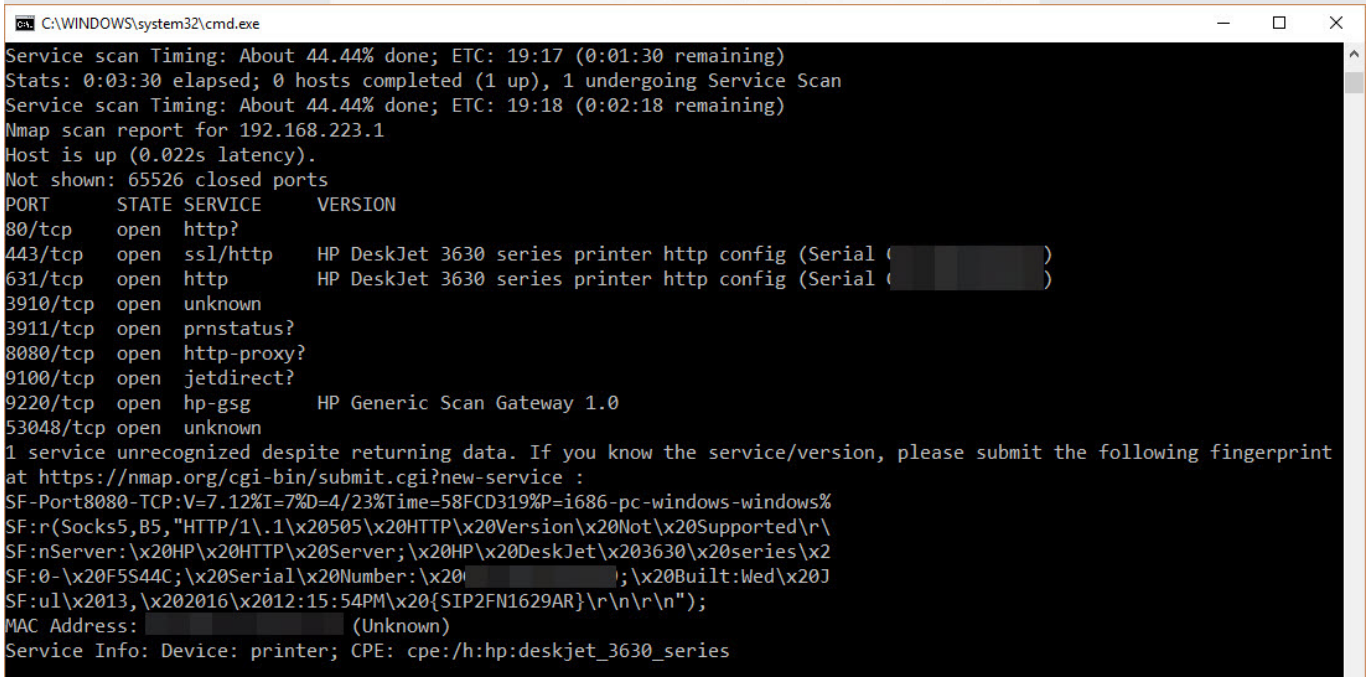




HP Scanner Thief aracı sayesinde eğer tarayıcı üzerinde bir işlem gerçekleştirildiyse ve 20 saniye içinde taranan belge yazıcıdan fiziksel olarak alınmadı ise dokümanın dijital olarak çalınması mümkün olabiliyor bu nedenle yönetim arayüzünden varsayılan Wi-Fi Direct parolasının güçlü bir parola ile değiştirilmesi büyük önem taşıyor!

Bu yazıdan ve çalışmadan çıkarmamız gereken ders, günümüzde alacağımız cihazları sadece fiyat ve performans açısından değil, güvenlik açısından da değerlendirip, satın aldıktan sonra üreticinin bize sunmuş olduğu kolay kurulum adımları, araçları ile yetinmeyip güvenliğini (güçlü parola, gereksiz servislerin kapatılması vs.) sağladıktan sonra cihazı ev veya iş ağımıza dahil etmek olacaktır.





Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.