Ettercap ile Password Sniff'leme

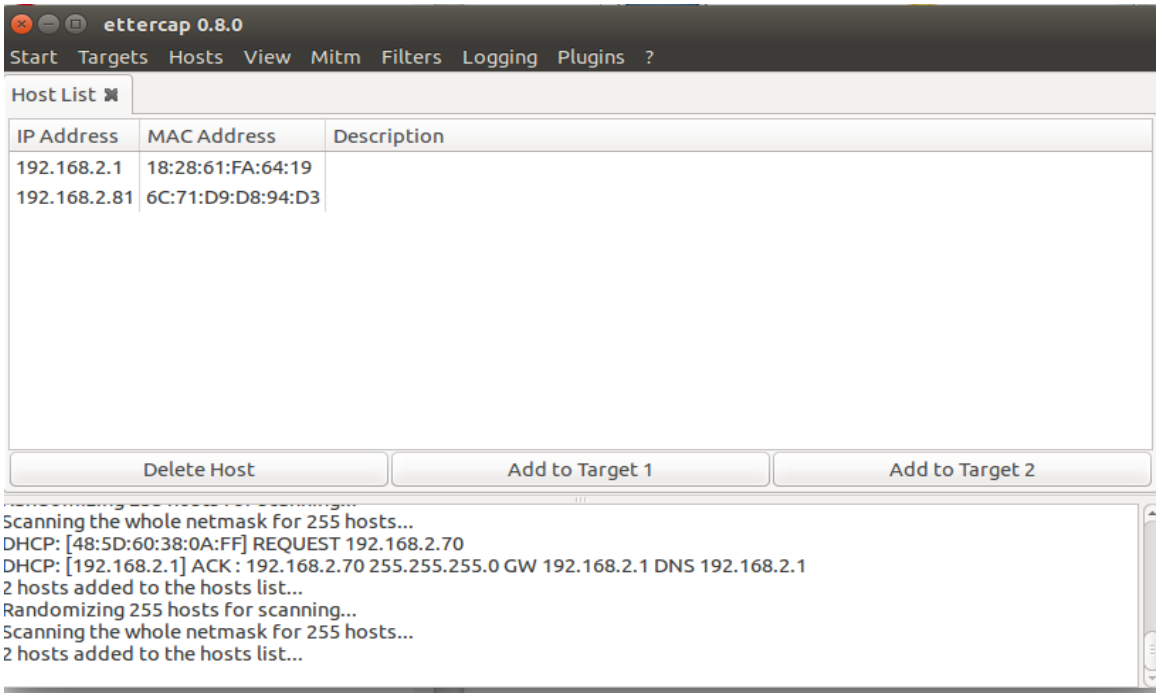
Ettercap'in GUI'ını konsoldan başlatalım.

> sudo ettercap -G

Ardından menü çubuğundan sırasıyla

Options->Promisc Mode
Sniff->Unified Sniffing
Hosts->Scan For Hosts

sekmelerine tıklayalım. Hosts->Hosts List sekmesine birkaç kere tıklanması iyi sonuçlar sunabilir. Bu host tarama işleminden sonra menüden Hosts->Hosts List sekmesine geçilerek network'te tespit edilen aktif cihazlar ekrana aşağıdaki gibi basılır.



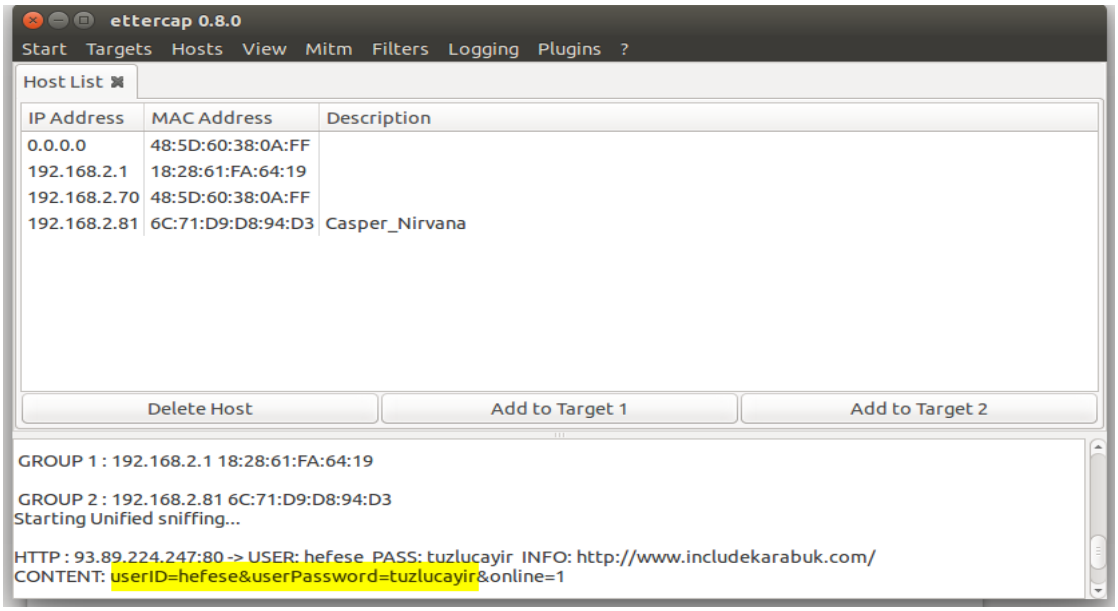
Eğer router'a ait IP' için Add to Target 1 butonuna tıklanırsa ve geri kalan tüm IP'ler için Add To Target 2 butonuna tıklanırsa network'teki tüm istemcilerin router'la olan trafiğini üzerimize almış oluruz.

NOT: 192.168.2.1 => Router'ın IP'si
192.168.2.81 => Annemin Laptop'ının IP'si

Diyelim ki router'a ait IP için Add To Target 1 butonuna, belirli bir istemcinin IP'si için de Add to Target 2 butonuna tıkladık. Sıradaki işlem Arp Poisoning işlemini başlatmaktır. Bunun için menüden MITM->Arp Poisoning sekmelerine tıklanılır. Ekrana gelen prompt'tan Sniff Remote Connections checkbox'ı seçilir ve OK diyerek geçilir. Böylece router ile hedef bilgisayarın (annemin laptop'ının) arasına girmiş oluruz. Bu işlem sonrası yapılacak şey üzerimizden akan trafiği

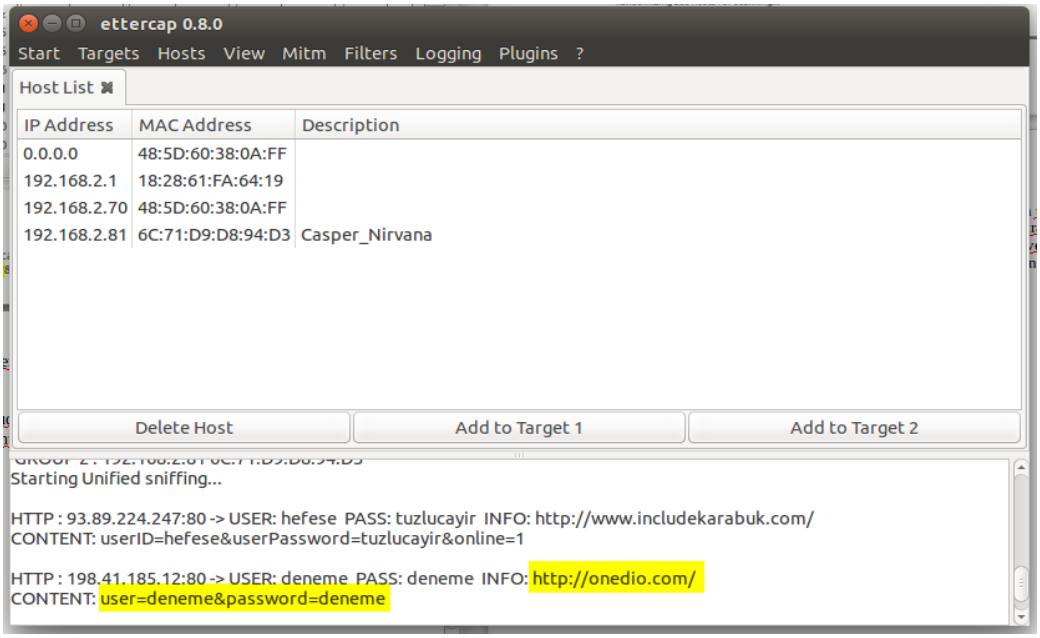
sniff'lemektir. Bunun için menüden Start->Start Sniffing sekmesine gelinir ve Ettercap penceresinin alt tarafındaki textarea gözlenmeye başlanır. Artık saldırgan hazır vaziyettedir ve kurbanın surf yapmasını bekleyecektir.

Şimdi hedef bilgisayardan (annemin laptop'ından) www.includekarabuk.com/adminPaneli/ sayfasına gidelim ve login ekranından giriş yapalım. Giriş yaptığımız anda saldırganın bilgisayarındaki Ettercap penceresinin alt tarafında yer alan textarea'da sniff'lenen includekarabuk'e ait kullanıcı adı ve şifre görüntülenecektir.



Görüldüğü üzere hedef bilgisayardan includekarabuk login ekranına girilen kullanıcı adı ve şifre saldırganın makinasındaki Ettercap tarafından sniff'lenmiştir ve GUI'ın alt tarafındaki textarea'da görüntülenmiştir.

Diyelim ki hedef bilgisayardan bu sefer onedio.com'a giriş yaptık. Bu durumda



yine textarea'dan görüleceği üzere kullanıcı adı olarak “deneme”, şifre olarak da “deneme” verisinin hedef bilgisayardan onedio'da oturum açmak için girildiği görülmektedir. Dikkat edersen Onedio'ya ait login bilgilerinin hemen üstünde daha önceki sniff'lenen includekarabuk sitesine ait login bilgileri yer almaktadır. Yani Ettercap'in penceresindeki bu textarea sniff'lenen trafikteki sadece kullanıcı adı ve şifrele verilerini cımbızlayıp ekrana yansıtan bir işleve sahiptir.

Sniff'in işlemi sonrası hedef bilgisayarı terk edebilmek için sırasıyla

Start->Stop Sniffing
Mitm->Stop Mitm Attack(s)

sekmelerine tıklanmalıdır. Böylece hedef bilgisayar tekrar rayına oturur ve hedef bilgisayarın internet bağlantısı sekteye uğramamış olur.

Sonuç

Hedef bilgisayardan yapılan iki oturum açma işleminde de Ettercap kullanıcı adı ve şifreyi sniff'leyebildi. Fakat eğer hedef bilgisayardan facebook gibi bir site için oturum açma denenseydi Ettercap'in textarea'sı kullanıcı adı ve şifreyi ekrana yansıtmayacaktı. Çünkü facebook https protokolüne sahip olduğundan uçtan uca şifreleme kullanmaktadır. Yani hedef bilgisayardan girilen kullanıcı adı ve şifre daha hedef bilgisayardan çıkmadan şifrelendiğinden ve sunucuya şifreli olarak gittiğinden aradaki saldırgan bu trafiği sniff'leyebilse bile anahtarı bilmediğinden şifreli veriyi anlamlandıramayacaktır. Dolayısıyla Ettercap şifreli karman çorman veri ekrana yansıtmak yerine hiç yansıtmamayı prensip olarak seçmiştir. Önceki örneklerde (includekarabuk ve onedio'da) şifrelerin sniff'lenebilmesinin nedeni bu sitelerin http protokolünü kullanıyor olmaları, yani uçtan uca şifreleme kullanmıyor olmalardır.

Ekstra

Enes'in sözü üzerine VPN kullanırken Ettercap ile sniff'leme yapılabiliyor muyu öğrenmek için enesin (kurbanın) makinesinde vyprVPN adlı VPN yazılımı açılmıştır ve Ettercap ile enesin makinası sniff'lemeye tabi tutulmuştur. Enesin makinasında VPN yazılımı açık olduğu durumda bir http protokolü kullanan login sayfasına girilen kullanıcı adı ve şifre bilgilerinin sniff'lenemediği görülmüştür. Yani ettercap'in arayüzüne hiçbir bilgi düşmemiştir. Ancak VPN yazılımı kapatıldığında ve aynı login sayfasına giriş yapıldığında kullanıcı adı ve şifre bilgilerinin sniff'lenebildiği görülmüştür. Enesin makinasında VPN yazılımı tekrar açık olduğu durumda bir başka http protokolü kullanan login sayfasına girilen kullanıcı adı ve şifre bilgilerinin yine sniff'lenemediği görülmüştür. VPN yazılımı kapatıldığında ve aynı login sayfasına tekrar giriş yapıldığında ise kullanıcı adı ve şifre bilgilerinin sniff'lenebildiği görülmüştür. Yani VPN varken Ettercap sniff'leyemiyor, VPN yokken Ettercap sniff'leyebiliyor. Demek ki VPN'ler tıpkı https protokolünü kullanan web sitelerin uçtan uca şifreleme yapması gibi bağlantıyı şifrelediğinden Ettercap programı kullanıcı adı ve şifre bilgilerini şifreli oldukları için ekrana düşürmüyor.

Kaynak : Tez Raporu/Literatür Taraması/İncelenmiş Makaleler/BGA/Pentest Çalışmalarında Kablosuz Ağ Güvenliği Testleri.docx , page 46-47