LLMNR
Ve
NetBIOS-NS Poisoning

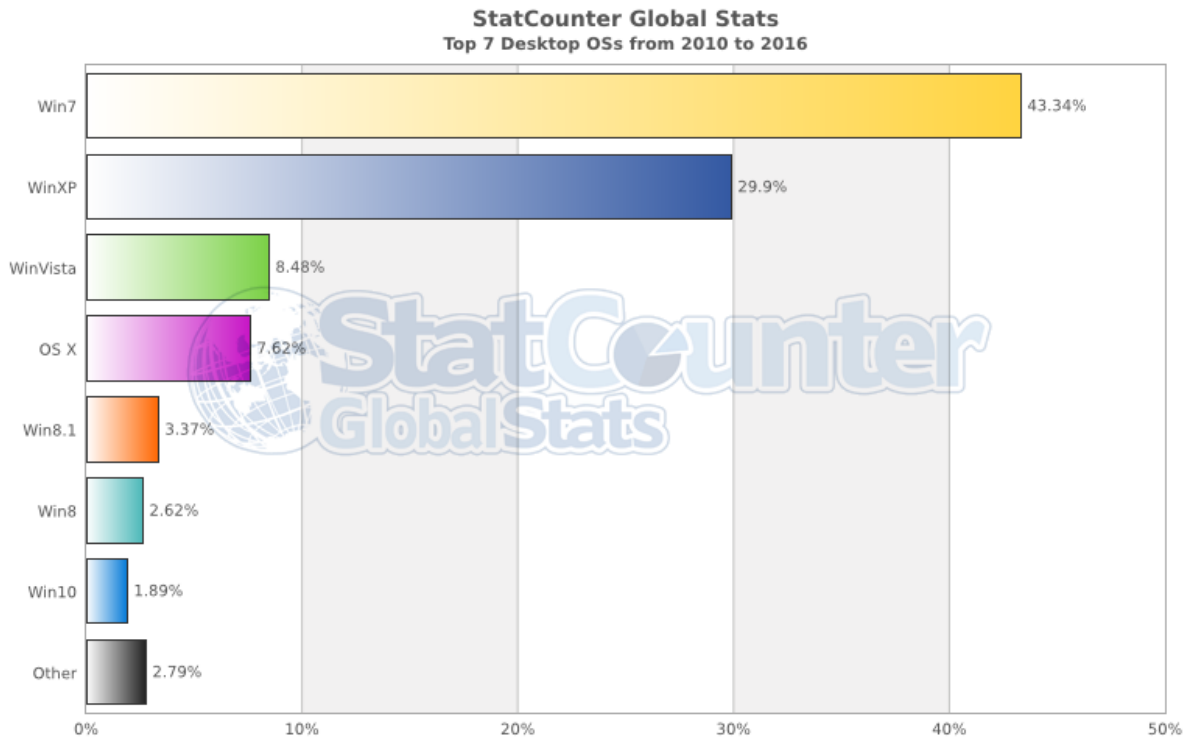
Yazar: Halil Dalabasmaz
Baskı: Aralık, 2016

Yerel ağda hedefin veya hedeflerin trafiğini ele geçirmek ve müdahale etmek için birden fazla yöntem bulunmaktadır. Bunların arasında ARP Poisoning en bilineni olup, en fazla istismar edilenidir. TCP/IP uzun yıldır var olan bir protokol ve ARP Poisoning, Rogue DHCP Server Attack vs. ise yine yıllardır yerel ağ trafiğine müdahale etmekte kullanılan saldırı yöntemlerinden bazılarıdır.

Gerçekleştirdiğim sızma testlerinde tecrübe ettiğimiz en önemli nokta; yerel ağlarda bu saldırı yöntemleri her zaman işe yaramamaktadır, çünkü ARP Poisoning DHCP Starvation vb. saldırı tekniklerinin önlemleri büyük oranda Switch üzerinde kolaylıkla alınabilmektedir. Günümüzde bilinçlenmenin artmasıyla "yıllardır" var olan TCP/IP protokolündeki, "yıllardır" istismar edilen/edilebilecek zafiyetler için ağ yöneticileri önlemlerini "almaktadır".

Bu noktada şöyle bir soru sorarsak yazıyı daha da anlamlandırabiliriz ve tam anlamıyla giriş yapabiliriz; *yerel ağ saldırıları (ARP Poisoning, DHCP Starvation, Rouge DHCP vs.) için tüm önlemlerin alındığı bir ağ içerisinde hedef veya hedeflerin ağ trafiğine nasıl müdahale ederiz veya hedefe nasıl arka kapı yerleştirebiliriz?*

Kurumsal ağlar içerisinde özellikle son kullanıcı tarafında Windows işletim sistemleri en çok kullanılan işletim sistemidir ve aşağıdaki grafikte örnek işletim sistemi kullanım dağılımı verilmiştir.



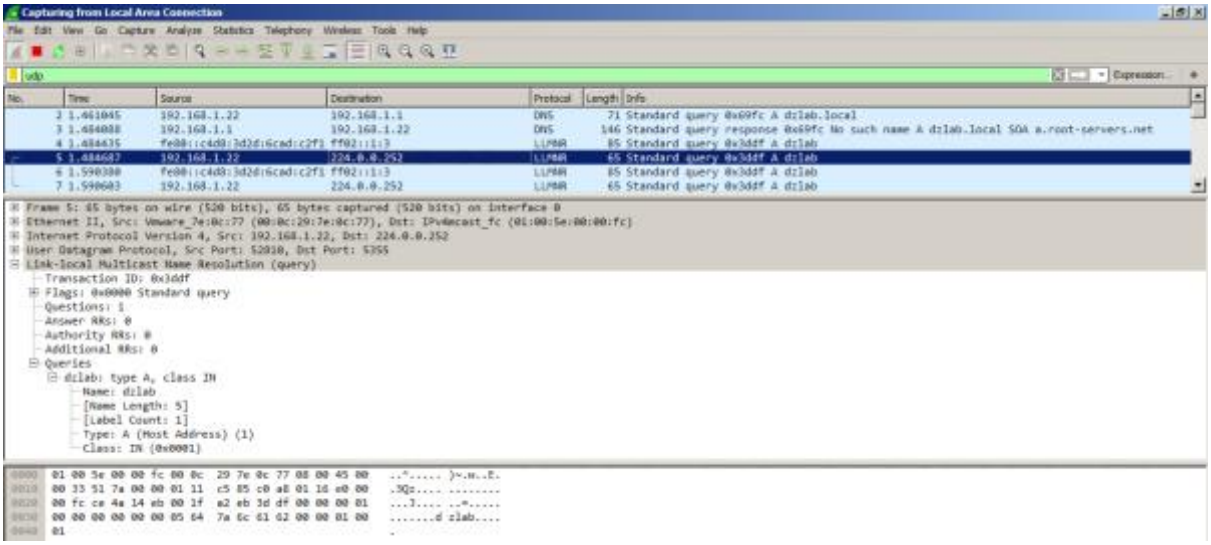
2010 – 2016 Arası Küresel İşletim Sistemi Dağılımı (*)

LLMNR Nedir?

LLMNR (Link-Local Multicast Name Resolution), IPv4 veya IPv6 üzerinden sistemlerin yerel ağdaki diğer sistemlerin isimlerini çözmek kullandıkları, temelde DNS tabanlı bir protokoldür. Yerel ağlar DNS'e alternatif olrak geliştirilen bir protokol değil, DNS sorgularının olumsuz sonuçladığı durumlarda kullanılmaktadır. Windows Vista sonrası tüm Windows işletimleri sistemleri tarafından desteklemektedir. Aynı zamanda 2014 sonlarına doğru Linux üzerinde de gerekli entegrasyon gerçekleştirilmiştir.[1]

Herhangi bir yapılandırmaya ihtiyaç duymadan sistemler LLMNR'ı kullanabilmektedir ve temelde DNS sorgularının işe yaramadığı durumlarda devreye girmektedir. LLMNR protokolü IPv4 üzerinde 224.0.0.252, IPv6 üzerinde ise FF02:0:0:0:0:0:1:3 link-scope multicast adresleri kullanır ve TCP/UDP üzerinde 5355 portu üzerinde işlemlerini gerçekleşmektedir.

Örnek olarak olmayan bir alan adına (dzlab.local) ping atmayı deneyelim. Başarısız sonuçlanan DNS sorgularının hemen ardından LLMNR sorguları oluşmaktadır. Aşağıda ilgili ekran görüntüsü verilmiştir.



LLMNR Sorguları

Özet olarak DNS üzerinden isim çözümlemenin mümkün olmadığı durumlarda işletim sistemi LLMNR protokolünü kullanıp ismi çözmeye çalışıyor.

NetBIOS Nedir?

[*] https://lwn.net/Articles/609740/

NetBIOS (Network Basic Input/Output System), yerel ağ içerisinde sistemlerin birbirleri arasında iletişim için kullandıkları bir API'dır. Bilinenin aksine bir protokol değil protokol üzerinde çalışan bir API'dır. Üç farklı servisi vardır;

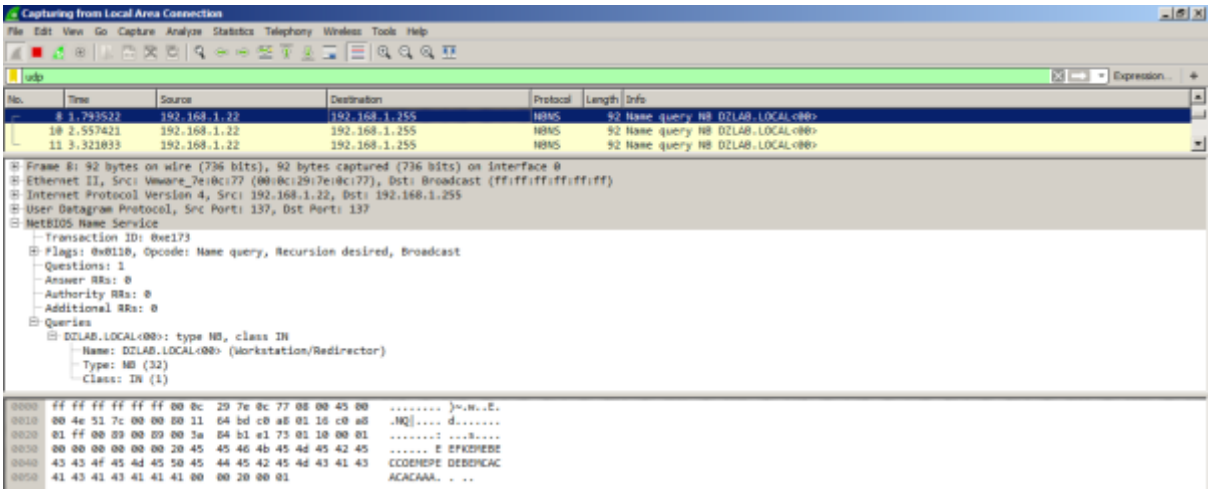
- *Name Service (NetBIOS-NS),* isim kaydı ve isim çözme için kullanılır. UDP 137 portundan işlemler geçekleştirilir. Aynı zamanda TCP 137 portu da bazen kullanılır.
- *Datagram Distribution Service (NetBIOS-DGM),* Connectionless iletişim için kullanılır. UDP 138 portunda işlemler geçekleştirilir.
- *Session Service (NetBIOS-SSN),* Connection-Oriented iletişim için kullanılır. TCP 139 portu üzerinden işlemler geçekleştirilir.

Windows İşletim Sisteminde İşler Nasıl Yürüyor?

Bir Windows işletim sistemi isim çözerken aşağıdaki adımları takip eder;

1. Sistemindeki hosts dosyasına bakar.
2. Yerel DNS Önbelleğine bakar.
3. DNS Sunucusuna sorgu gönderir.
4. LLMNR sorgusu gönderir.
5. NetBIOS-NS sorgusu gönderir.

Yukarda, "dzlab.local" için ping atmaya çalışmıştık DNS sunucusu üzerinden kaydı olmayan bu domain için DNS sorgusu oluşmuştu ardından LLMNR isteği ve hemen sonrasında NetBIOS-NS isteği oluşmuştu. Aşağıda NetBIOS-NS isteğinin detaylarını içeren ekran görüntüsü verilmiştir, ilgili paketin DST kısmına bakılırsa bunun broadcast bir paket olduğu ve yerel ağdaki tüm sistemlere gönderildiği anlaşılabilir.



NetBIOS-NS Sorguları

Bu paket broadcast bir paket ise herhangi bir sistem bu pakete cevap verebilir diyebiliriz. Normal şartlar altında cevabı bilen sistem kaynak sisteme cevabı döner. Ancak kimse bilmiyorsa istek öylece yanıtsız kalır. Eğer sorulan alan adı gerçekten varsa doğru cevabı bilen

sistemler arasından hangisinin cevabı öncelikle soran sisteme ulaşırsa o işlenir. Kısaca doğru cevaplar için bir "race condition" durumu söz konusudur.

İşte tam bu noktada bu isteklere saldırgan olarak cevap verebilir ve hedef sistem ile ilgili hassas verilere erişebilir, başka bir yere yönlendirebilir hatta hedefe arka kapı bile yerleştirilebilir. Temelde yapılacak olan şey broadcast gelen paketleri dinlemek ve onlara gerektiği şekilde cevap vermektedir.

Bu işlemler için Kali işletim sisteminde kurulu olarak gelen veya GitHub üzerinden erişlebilecek (https://github.com/SpiderLabs/Responder), açık kaynak kodlu Responder isimli araç yazı içerisinde kullanılmıştır.

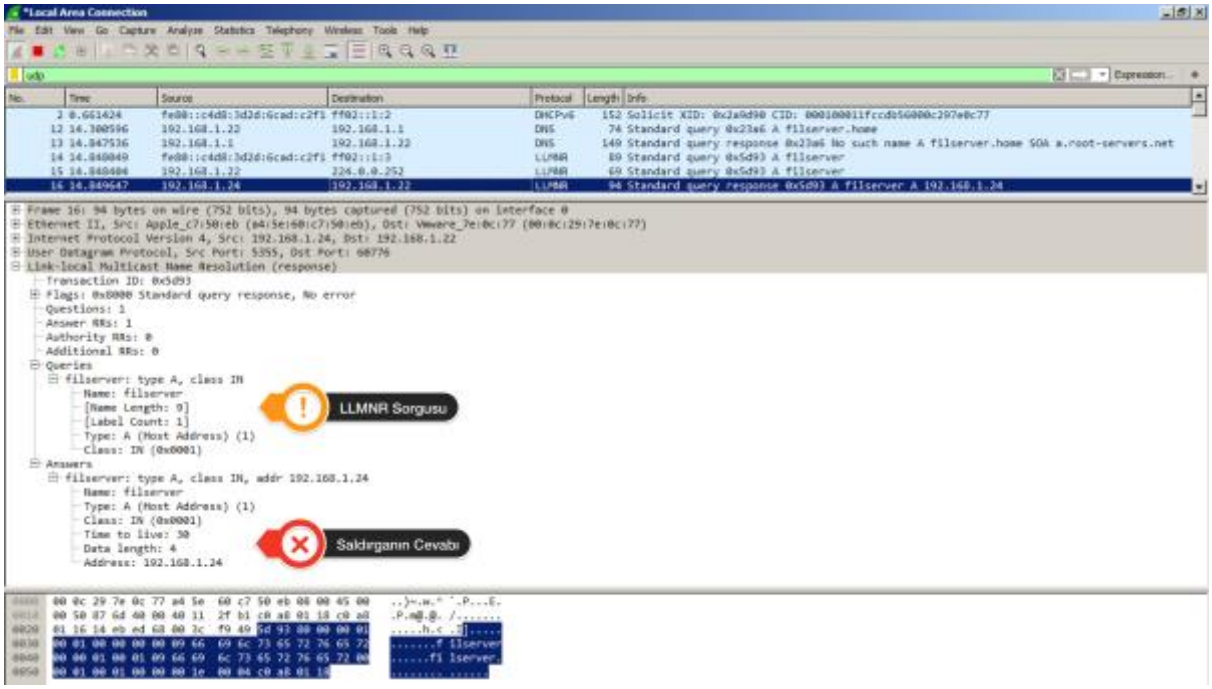
Hedefin NTLMv2 Hash'ini Ele Geçirme

Araca herhangi bir parametre vermeden direkt olarak ağ arayüzünü tanımlayarak çalıştırdığımızda gelecek olan LLNMR ve NetBIOS-NS isteklerini dinlemeye başlayacaktır.

```
$ responder -I eth0
```

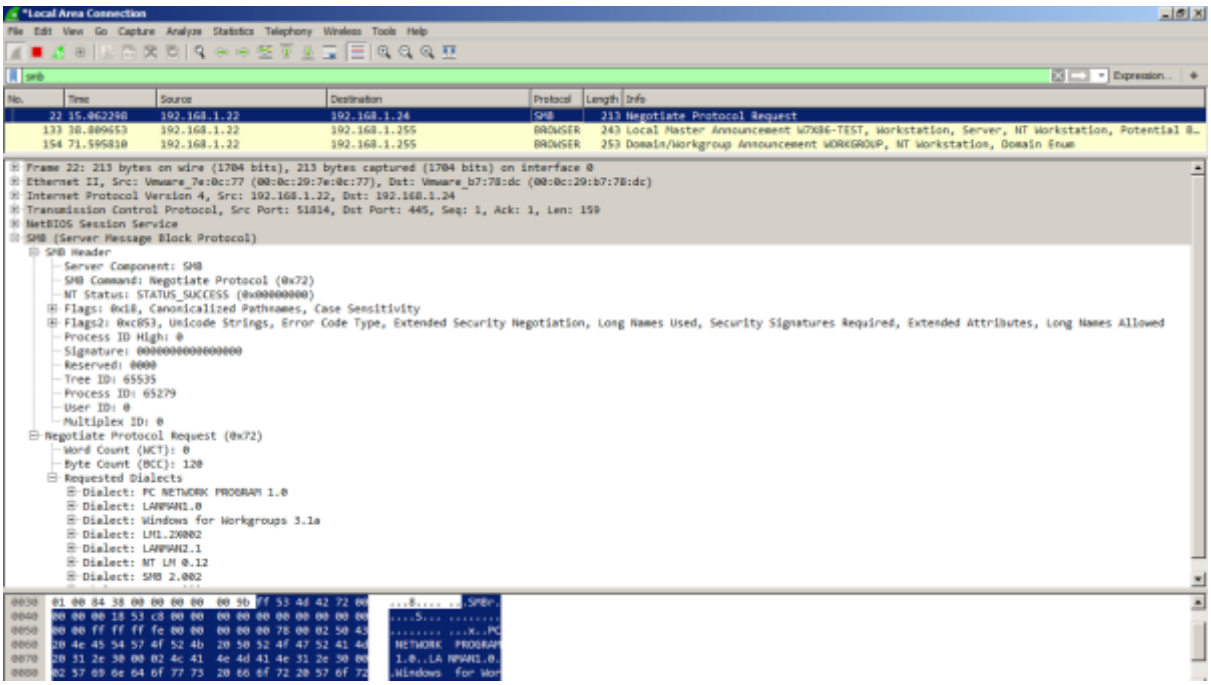
Örnek vererek ilerlersek;

- Kullanıcı aslında \\fileserver\'a erişmek istiyor ancak yanlış yazıp \\filserver\ şeklinde yazarak erişmeye çalışıyor.
- Bu durumda kaydı bulunmayan ilgili sistem için sorgular başlıyor. Saldırgan gelen LLMNR isteklerine cevap veriyor ve kendisinin \\filserver\ olduğunu cevap olarak dönüyor.



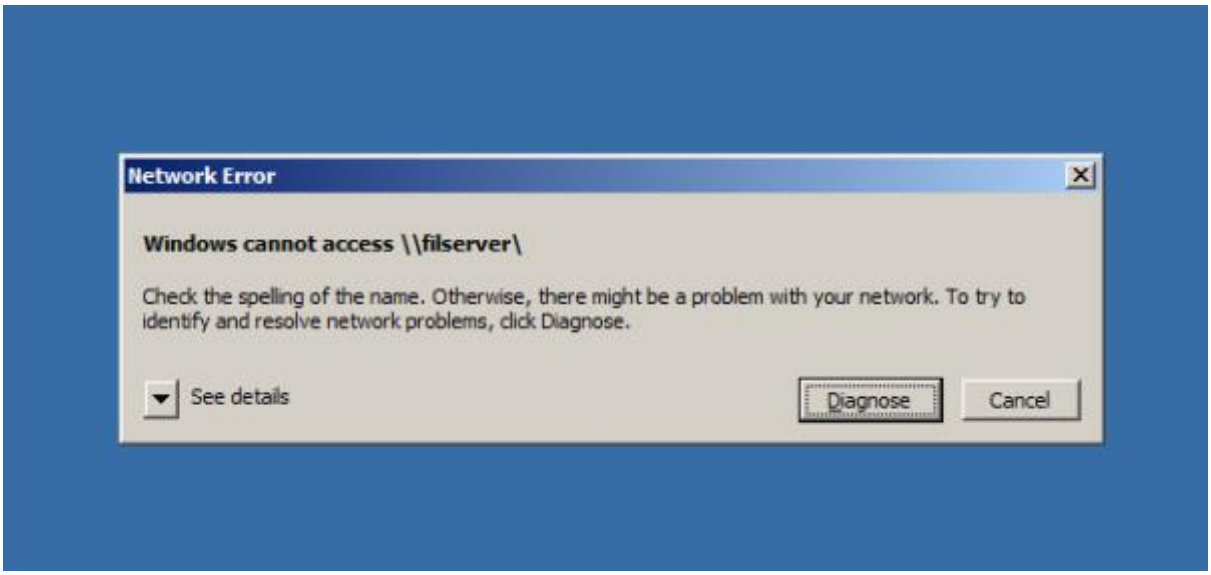
filserver İçin Oluşan Sorgu ve Cevap

- Kullanıcının işletim sistemi bağlantı kurup o an oturumu aktif olan kullanıcı adı ve NTLMv2 hash (parola özetini)'ini saldırgana veriyor.



Bağlantı Paketi

- Hedef bağlantı hatası ile karşılaşıyor.



Hedefin Aldığı Hata

- Saldırgan hedefin NTLMv2 parola özetini ele geçiyor.

İsteğin Zehirlenmesi ve NTLMv2 Hash'in Elde Edilmesi

Bu noktadan sonra saldırgan hedeften elde ettiği NTLMv2 hashi kırarak diğer saldırı aşamalarına geçilebilir. Çünkü NTLMv2 hash'i Pass The Hash vb. herhangi bir yöntem için kullanılamamaktadır.

Hedeften Açık Hesap Bilgisi Elde Geçirme

WPAD (Web Proxy Auto-Discovery Protocol), yerel ağ içerisinde veya internete erişim için proxy ayarının gerektiği durumlarda, proxy ayarlarının otomatik olarak istemcilere gönderilmesi ve işletilmesi için kullanılan teknolojidir. Proxy adres veya adresleri "wpad.dat" dosyası içerisine eklenir ve istemcilere DHCP veya DNS üzerinden almaları sağlanabilir. Örnek wpad.dat içeriği aşağıda verilmiştir.

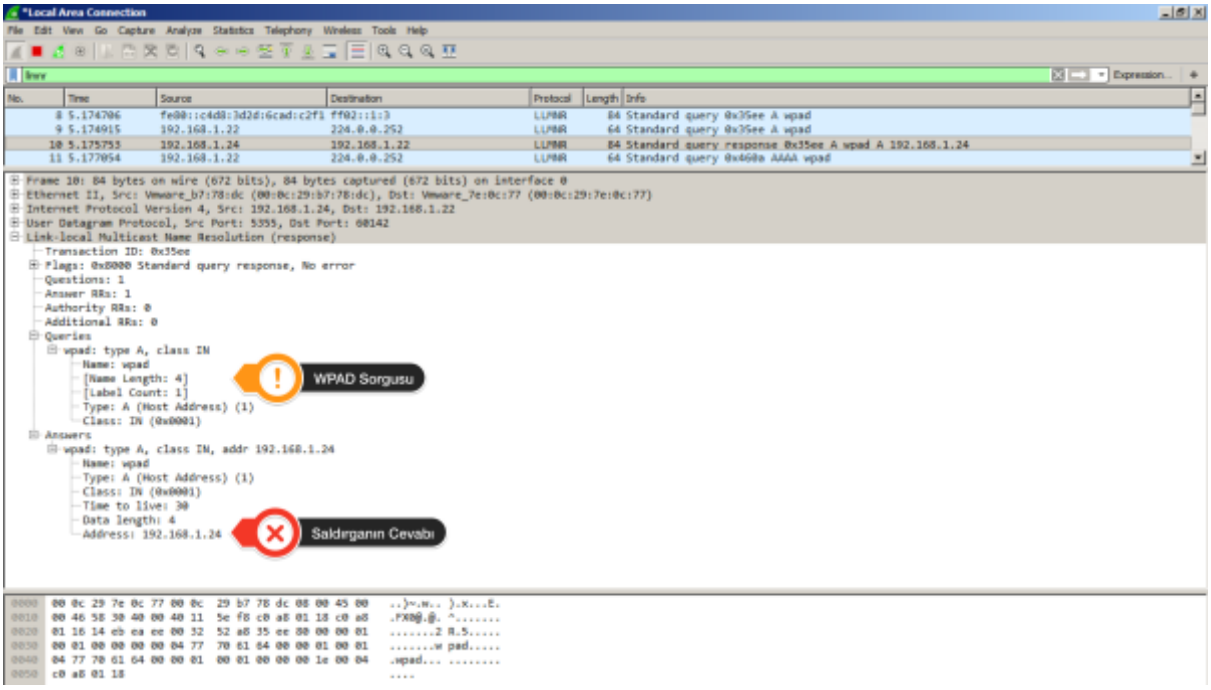
```
function FindProxyForURL(url, host)
{
     return "PROXY proxy.example.com:8080; DIRECT";
}
```

WPAD aşağıdaki gibi çalışmaktadır;

1- DHCP ayarları yapıldıysa istemci DHCP üzerinden WPAD bilgisini alır. (Başarılı ise 4. adıma geçilir.)
2- DNS'e "wpad.<corpdomain>.com" sorulur. (Başarılı ise 4. adıma geçilir.)
3- WPAD için LLMNR sorgusu gönderilir. (Başarılı ise 4. adıma geçilir. Başarısız ise proxy kullanılmaz.)
4- "wpad.dat" dosyası indirilir ve içerisinde bulunan proxy ayarları sistemde kullanılmaya başlanır.

Normal şartlarda birinci adımdaki istek üzerinden hedefe saldırı gerçekleştirilmek isteniyorsa DHCP Spoofing saldırısı deneneblilir ya da ikinci adımdaki istek üzerinden hedefe saldırı gerçekleştirilmek isteniyorsa DNS Poisoning saldırısı denenebillir. Ancak yukarıda da değinildiği üzere bu tür saldırılarına alınan önlemlere karşı neler yapabilir konusuna değindiğimiz için, amaç hedef üçüncü adıma geldiğinde neler yapılabilirdir.

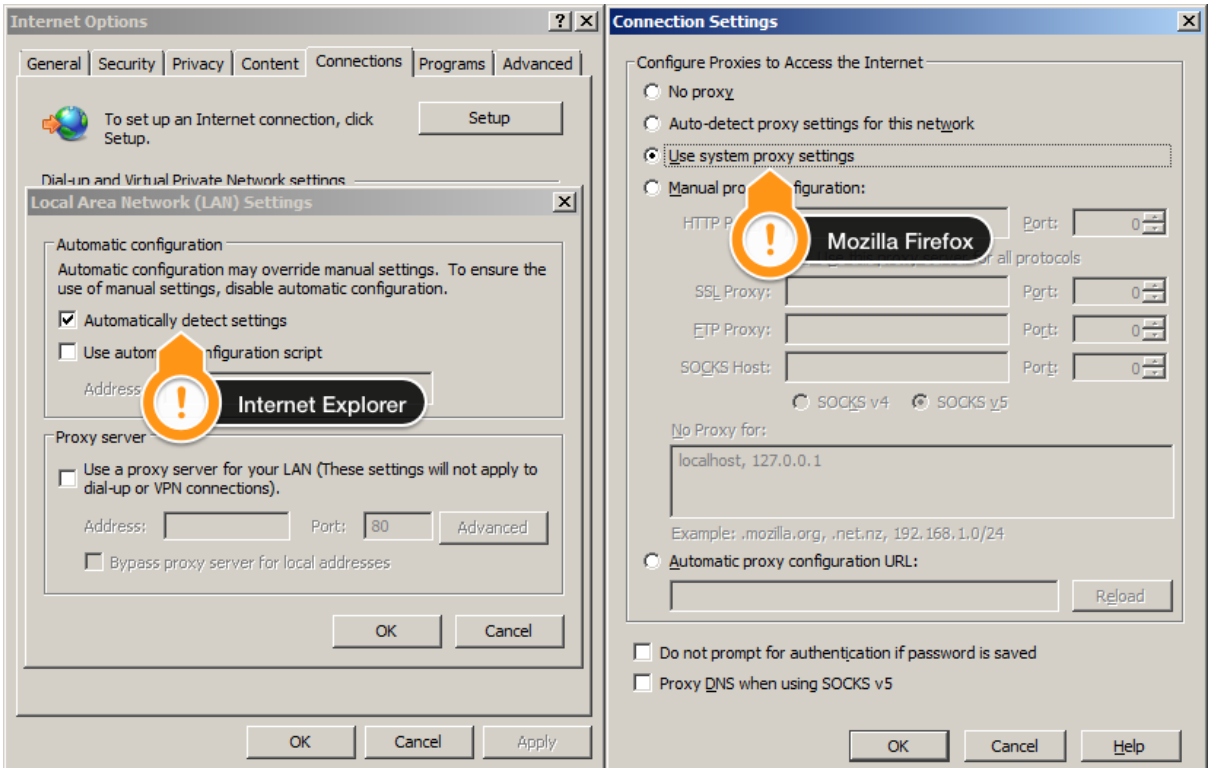
LLMNR üzerinden WPAD sorgusu gerçekleştiğinde ağ içerisindeki her istemciye bu istek gidecektir. Saldırgan bu noktada gelen WPAD isteğini zehirleyip (Sahte WPAD Sunucusu gibi hareket ederek) hedefe kendi oluşturduğu "wpad.dat" dosyasını vererek saldırıyı gerçekleştirebilir.



İsteğin Zehirlenmesi ve Saldırganın Cevabı

Bu saldırı türünde saldırganın avantajı olan bir durum söz konusu; Windows işletim sisteminin temel tarayıcısı Internet Explorer'ın proxy ayarları varsayılan olarak kurumla beraber "Automatically detect settings" şeklindedir.

Aynı zamanda Mozilla Firefox tarayıcısının proxy ayarları varsayılan olarak kurulum ile beraber "Use system proxy settings" şeklinde olup Chrome tarayıcısı da Internet Explorer üzerinden yapılan proxy ayarlarını kullanmaktadır.



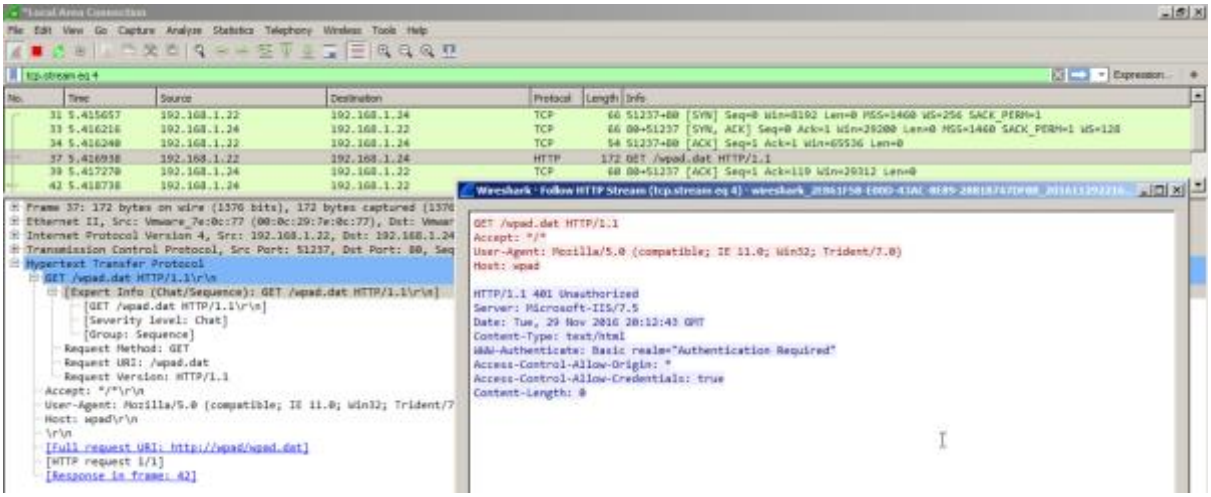
Internet Explorer ve Mozilla Firefox Proxy Ayarları

Saldırı için kullanılacak araç olan Responder aşağıdaki parametreler için çalıştırıldığında kendisine gelen WPAD paketlerine cevap dönecektir ve döneceği cevap proxy için yetkilendirmenin (Basic Authentication) gerektiği anlamına gelecektir.

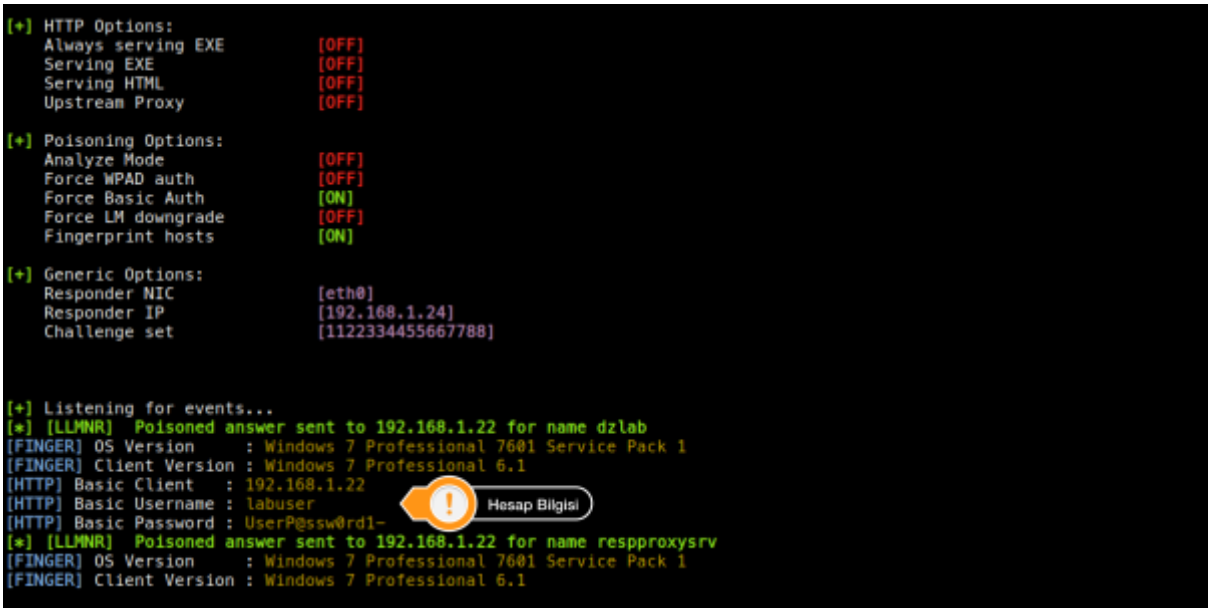
```
$ responder -I eth0 -wFb
```

Kullanıcı tarafında kullanıcı adı ve parola girilmesi için bir ekran çıkacaktır. Bu aşamada kullanıcının gireceği değerleri açık (clear-text) olarak saldırgan ele geçecektir ve genelde saldırıya maruz kalan kullanıcılar Windows kullanıcı hesaplarının bilgilerini girmektedir.

Karşılaşılan Basic Authentication Penceresi



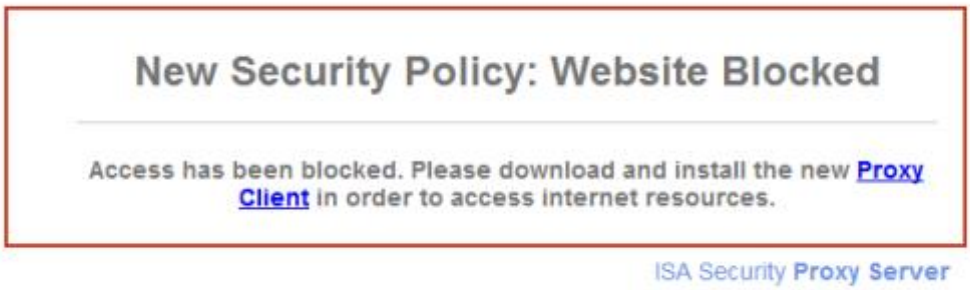
WPAD.DAT Dosyasına Erişim İsteği ve Cevabı



İsteğin Zehirlenmesi ve ClearText Hesap Bilgisinin Elde Edilmesi

Hedefe Arka Kapı Yerleştirme

Yukarıda WPAD isteklerine cevap dönerek hedeften açık (clear-text) olarak hesap bilgisinin nasıl alınabileceğine değinmiştim. Bu durumu bir adım öteye taşıyarak kullanıcının oluşturduğu isteği belirli bir sayfaya yönlendirerek kullanıcıya çalıştırılabilir dosya indirmesini sağlayabiliriz. Bu noktada oluşturulacak sayfanın inandırıcılığı için biraz sosyal mühendislik becerisi gerekmektedir ancak Responder aracının içerisindeki varsayılan sayfa bu işlem için gayet başarılıdır.



Varsayılan Phising Sayfası

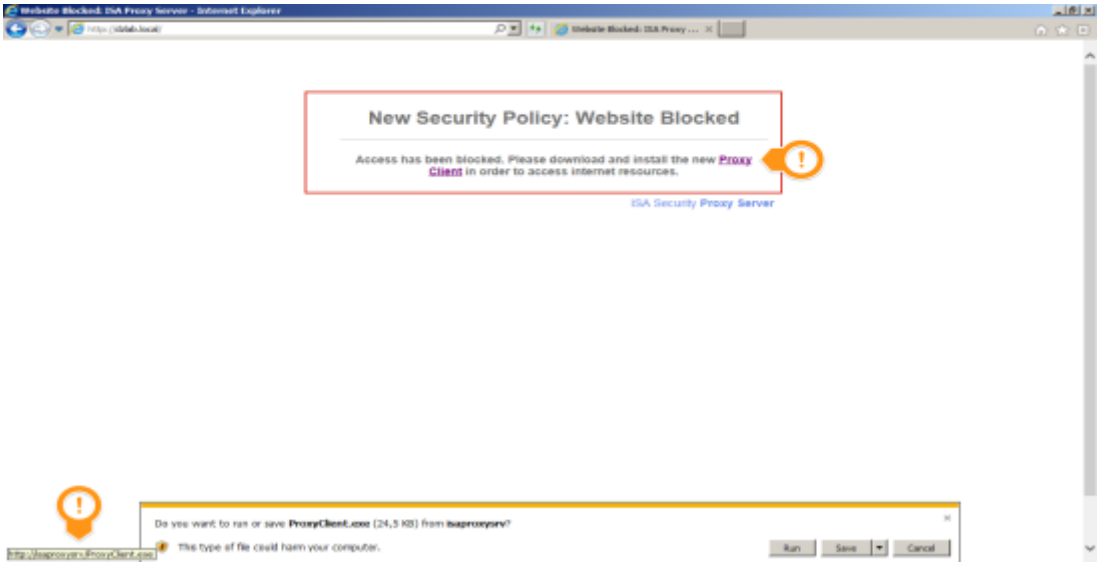
Responder aracının "/etc/responder/Responder.conf" dosyası içerisinde aracın yapılandırma parametreleri bulunmaktadır. Dosya içerisinde "Serve-Html" ve "Serve-EXE" parametreleri varsayılan olarak "Off" değerindedir. Öncelikle bu değerleri "On" olarak değiştirmemiz gerekmektedir.

```
[HTTP Server]

; Set to On to always serve the custom EXE
Serve-Always = On

; Set to On to replace any requested .exe with the custom EXE
Serve-Exe = On

; Set to On to serve the custom HTML if the URL does not contain
.exe
; Set to Off to inject the 'HTMLToInject' in web pages instead
Serve-Html = On
```

Ayarlar tamamlandıktan sonra Responder aracı aşağıdaki parametreler ile çalıştırıldığında gelen WPAD isteklerine cevap dönecektir ve cevapları işleyen istemciler saldırıya maruz kalacaklardır.

```
$ responder -I eth0 -wr
```

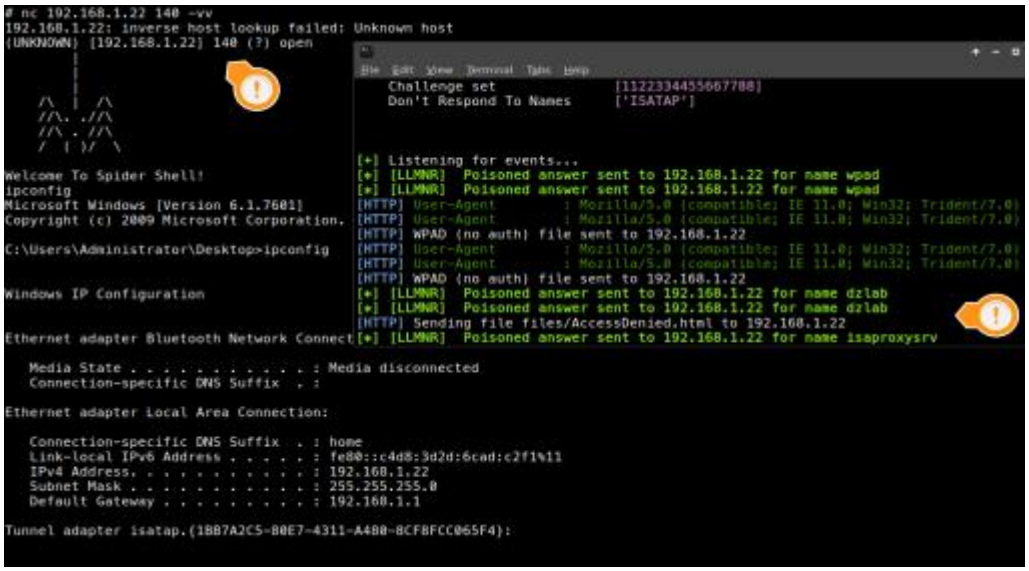
Saldırıya maruz kalan kullanıcılar aşağıdaki ekran görüntüsünde olan sayfa ile karşılaşacaklardır.



Karşılaşılan Sayfa ve Payload'ın İndirilmesi

Sayfada linki bulunan ProxyClient.exe dosyası hedef tarafından indirilip çalıştırıldığında TCP 140 portuna cmd.exe'yi bind edilecektir ve hedef üzerinde komut çalıştırılacak duruma geçilecektir.

Hedef kullanıcılar tarayıcılarından nereye gitmek isterlerse karşılarına "/usr/share/responder/files/AccessDenied.html" dizin yolundaki dosya verilecektir ve ilgili HTML dosyası içerisinde erişim için "ProxyClient.exe" isimli dosyayı indirip çalıştırmaları istenmektedir. "ProxyClient.exe" dosyası "/usr/share/responder/files/BindShell.exe" dizini yolunda bulunmaktadır ve istenirse başka çalıştırılabilir dosyalarda oluşturulup ilgili dizine atıldıktan sonra yapılandırma dosyası güncellenirse Responder aracı hedefe ilgili dosyayı verecektir.



İsteğin Zehirlenmesi ve Bind Shell'e Erişimi

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu" , "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.