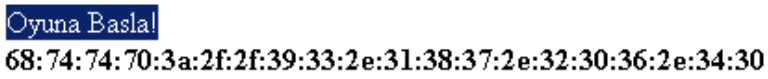
http://hackme.lifeoverip.net adresinde 30 Aralık 2009'da açılan Online CTF Yarışmasının Çözümleri.

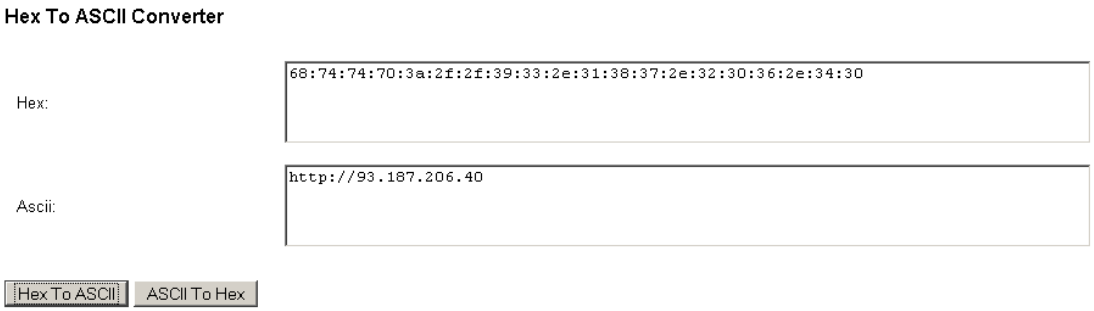
Yarışmaya katılan tüm ekiplere teşekkürler.

Yarışmada TurkGuvenligi ve YahsiBat1 ekipleri en yüksek puanı almış olup sonuç için gerekli olan 900 puana ulaşan takım olmadığı için yarışmayı –belirtilen kurallara uygun- kazanan olmamıştır.

Ön Eleme:



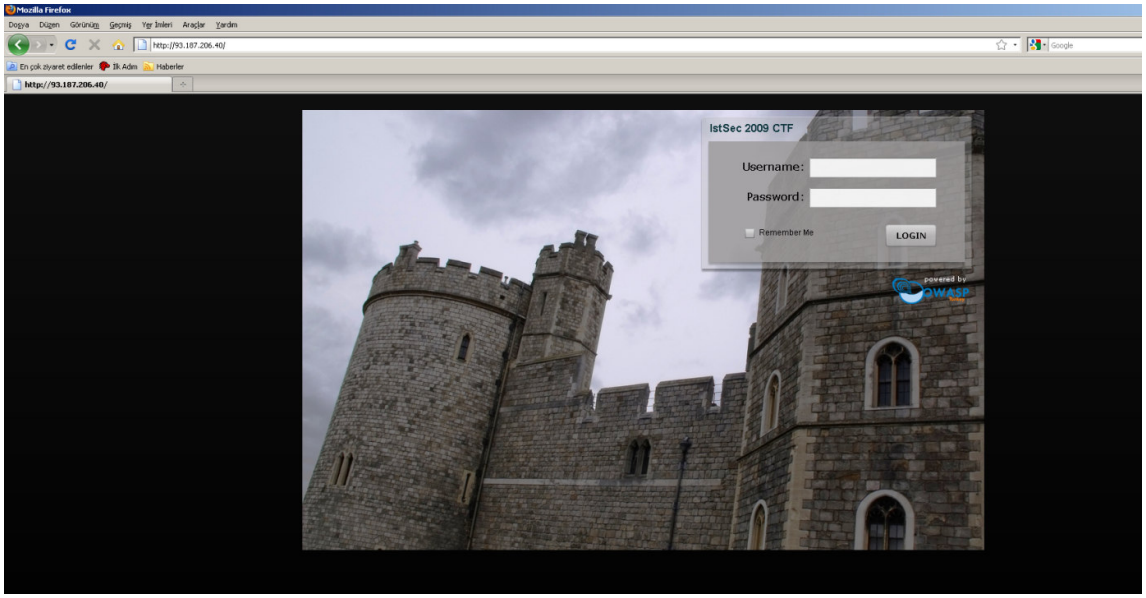
Çözümü: Herhangi bir HEX converter kullanarak yukardaki hex'i ascii'e çevirelim



Ascii olarak yazan ip adresi yarışmanın ilk adımına götürmektedir.

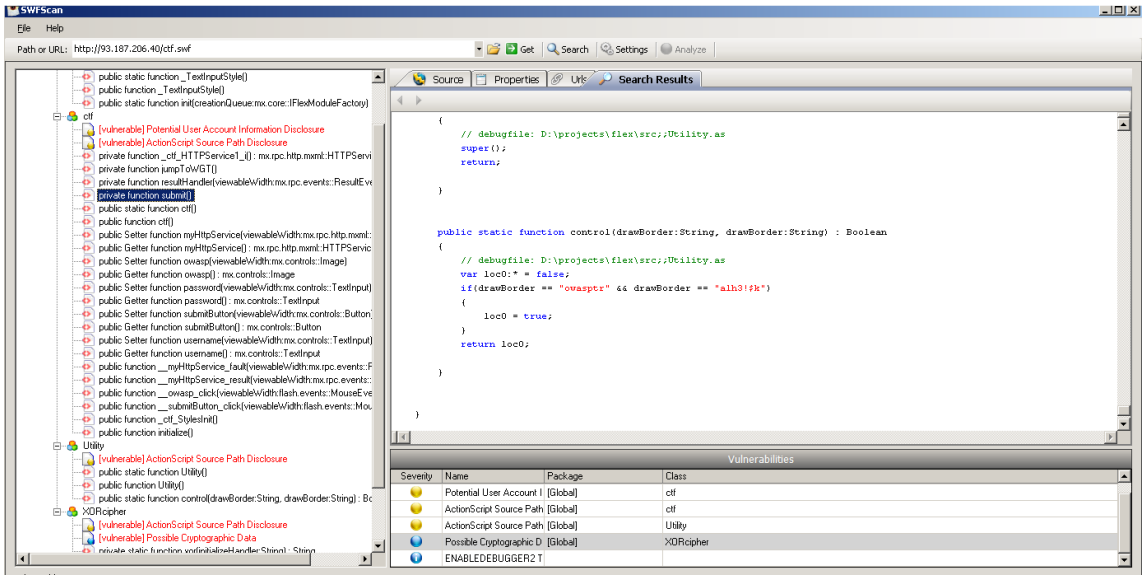
İlk Adım: Flash dosyasında user/pass bilgilerini girerek bir sonraki adıma ulaşmak.

Burada user/pass flash dosyasının içerisinde saklanmaktaydı ve yarışmacı her girdiği user/pass değerlerinde sanki sunucuya istek gidiyormuş gibi fake istekler yapıyordu.



Beklenen yarışmacının flash dosyasını çözümleyerek doğru user/pass bilgilerini girmesiydi.

SwfScan : http://www.hp.com/go/swfscan aracı ya da herhangi bir flash decompiler kullanılarak geçilecek bir adım.



Kullanıcı adı ve parola doğru girildikten sonra aşağıdaki sayfa gelecektir.

Online CTF oyununun birinci adimini gectiniz, puan tablonuzu guncellemek icin CTF@lifeoverip.net adresine "CTF Step1 Success" konu basligiyla mail gonderiniz

Mail icerigine takim isminizi yazmayi unutmayiniz!

Ikinci adim icin ipucu buralarda bir kutunun icinde gizlenmis olmali, kutu nerede acaba?

Sayfanın kaynağına bakıldığında aşağıdaki satırlar görülecektir.

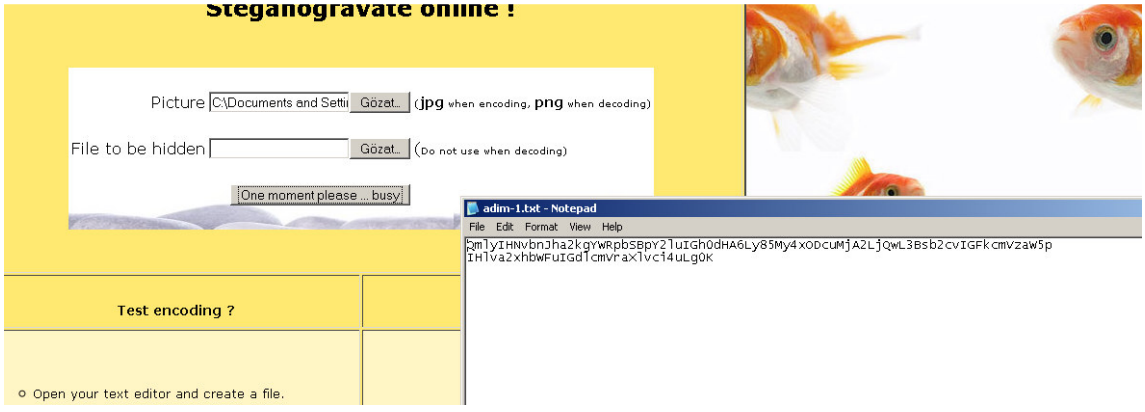
"<!-- Bir sonraki adim bu kutunun icerisinde http://93.187.206.40/steganography.png -->

<!-- Kutuyu acamazsaniz 10 puana hangi anahtarla acacaginiza dair ipucu satabilirim, ctf@lifeoverip.net -->

" Burada kutu resminin ismi bir ipucu olarak yer amlaktadır. Yani bir sonraki adım kutunun içerisine steganography ile gömülmüştür. Kutuyu açmak için uygun steg. Aracı bulunmalıdır.

Internette yapılacak "online steganography " araması ile kutunun içerisindeki şifre çözülebilecektir.

Bu adımda 10 puanlık ipucu verilmiştir(hangi steg. Aracını kullanacağını bulamayanlar için)



Kutu çözüldükten sonra içinden çıkan yazı base64 ile encode edilmiştir. Bunu da çözmek için herhangi bri base64decoder iş görecektir.

Evett. Bir sonraki adımın ne olduğunu da öğrendik. Devam edelim.

İkinci Adım

Bu adım biraz zorlu biraz da kafa karıştırıcı bir adımdı. Öncelikle sizi bir Wordpress sayfası karşılıyor, bu sayfa bazı ek alt sayfalara sahip olmasıyla birlikte kendisi de çeşitli güvenlik açıklıklıkları içermekteydi fakat bu açıklıkları exploit etmek bayağı zor bir adımdı. Amaç alt sayfalardaki açıklıkların bulunmasıydı.

Alt sayfalarda iki önemli ve basit açıklık vardı;

Bunlardan ilki galeri sayfasıydı ki burada sisteme resim upload ederek oylama yapılabiliyordu. Galeri sayfasındaki açıklık resim içerisine PHP kodu gömülerek sistemde çalıştırma idi. Buradan bir resim upload edip sistemde shell alınması ve bu sehll kullanarak sonraki adımlara ulaşılması bekleniyordu.

Diğer basit adım da **/phpmyadmin/** in sistemin alt dizinlerinde gizli olarak beklemesiydi(yani ana sayfadan link yoktu, sizin denemeniz gerekiyordu). Burada **/phpmyadmin** deneyenler bu sayfaya ulaşamadılar, /phpmyadmin/ deneyenler ise (Turkguvenligi ekibi) sayfaya ulaştı.

Phpmyadmin'de root parolası root(ya da boş) olarak bırakılmıştı. Buradan girerek sistem üzerinde işlem yapılabilirdi. Aslında phpmyadmin diğer adımları gereksiz kılan bir

kısayoldu yani bu adımı bulan biri ne steganography ne de flash dosyasını çözmeyle uğraşmayacaktı. Doğrudan veritabanını inceleyerek kurulu olan WP'nin yolunu bulabilirdi.

Her iki adımdan birini kullanarak sistemde komut çalıştıran ekipten beklenen root haklarına geçerek /root dizininde yazılı mesajı okumalarıydı. Root dizininde yazılı mesaj son adıma dair ipucu içermektedir.

Burada sistemde shell açılmaması için basit önlemler alınmıştı.

Bir sistemde shell açabilmek için sık kullanılan netcat aracı sistemden silindi, sistemde açık olan portlar harici ek port açılamıyordu ki bu da açılacak olan shellin mutlaka reverse shell olmasını gerekli kılıyordu. Reverse shell açmak için de sadece sistemden dışarı doğru 21, 80 ve 443. Portlar açıktı. Yani makine sizin açtığınız reverse shelli kullanabilmek için bu portlardan çıkış yapabilmekteydi.

Ek olarak sistemde local root exploit denenmesi gerekecekti(/root dizinindeki dosyayı okuyabilmek için). Sistem FreeBSD 8 ve rtld bug'ı güncellenmemiş(basit bir exploit ile root olunabiliyor). Burada sistemde exploitlerin derlenememesi için gcc ve buna bağlı derleyiciler sistemden kaldırılmıştı. Yarışmacılardan beklenen kendi sistemlerinde(freeBSD 8 kurulmuş olmalı) bu exploiti derleyerek binary dosyaları sunucuya atmalarıydı.

Ekiplerden biri bu adımı başardı ve sistemde root oldu, sonra onun attığı binary dosyaları kullanarak başka ekipler de sistemde root olmayı başardı☺.

Sistemde root olan ekip aşağıdaki dosyayı okudu ve sonraki adım için çalışmalara başladı:

 # ls -l /root/ctf_ikinciadim.txt

-rwx------ 1 root wheel 308 Dec 31 20:44 /root/ctf_ikinciadim.txt

 # cat /root/ctf_ikinciadim.txt

Heyyo! 250 puan aldiniz!

Bir sonraki adim icin root parolasini bularak, bu dizindeki sifrelenmis dosyayi okumaniz gerekiyor. Dosta 3des ile sifrelenmistir...

Root parolasi ayni zamanda bu dizindeki sifrelenmis dosyasin da parolasidir. Son adima az kaldi...

Root parolasini resetlersen bu dosyayi cozemezsin!

Evet root parolasının açık hali istenmekte ve bu bir sonraki adımı gösteren dosyanın anahtarı olarak saklanmakta. Burada yarışmacılar root olduktan sonra parolayı değiştirmiş olsalar diskalifiye olacaklardı zira root parolasıyla şifrelenmiş dosyayı başka türlü açamazlardı.

/etc/master.passwd dosyasından root parolasının hash'inin çözülmesi:

root:1nfNDTkFq$elEDWaxC0uh/u8qUSPvhm/:0:0::0:0:Charlie &:/root:/usr/local/bin/bash

Bu adım için en sık kullanılan araç John The Ripper, parolanın 9 karekterden oluştuğu ve sadece rakmalardan oluştuğu ipucu olarak yarışmacılara verildi.

Bundan sonraki adım 9 haneli üm olasılıkların değerlendirilmesiydi ki bu normal bilgisayar sistemlerinde bir haftadan daha fazla sürebilecek bir işlemdir.

Burada yarışmacılardan beklenen alternatif çözümlere yönelmeleri ya da password kırma işlemini paralel olarak gerçekleştirmeleriydi.

Eğer password kırma işlemine 00000000, 111111111, 222222222 şeklinde devam edilirse kırma işlemi oldukça zaman alacaktı. Kırma işleminde her bir karekter aralığı farklı makinede denenirse çok daha hızlı çözüm alınabilirdi(Mesela kırma işlemine 9 ile başlayanlar çok daha kısa sürede çözüme ulaşmış oldular).

Burada koyulan basit bir engel de john aracının incremental(x karekterli tüm olasılıkları on the fly deneme özelliği) olarak password kırma limitinin 8 olduğuydu. Yani 8 karekterden daha büyük parolalar inc yöntemle krılamıyordu, bir wordlist dosyasına ihtiyac duyuyordu. Bu adım john'u tekrar derleyerek aşılabilirdi ama her iki ekip de buna gerek duymadan çok kısa sayılabilecek sürede parolayı kırmayı başardılar.

Parolayı kırdıktan sonra aynı parolayı kullanarak /root/gizlimesaj dosyasını çözmek gerekiyordu. Bu dosya 3des ile şifrelenmiş ve parolası root parolasıyla aynı.

Aşağıdaki komut kullanılarak dosya içerisinde yazan ipucu okunabilir.

openssl enc -d -des3 -in gizlimesaj -out SONUC

enter des-ede3-cbc decryption password:

Son Adım

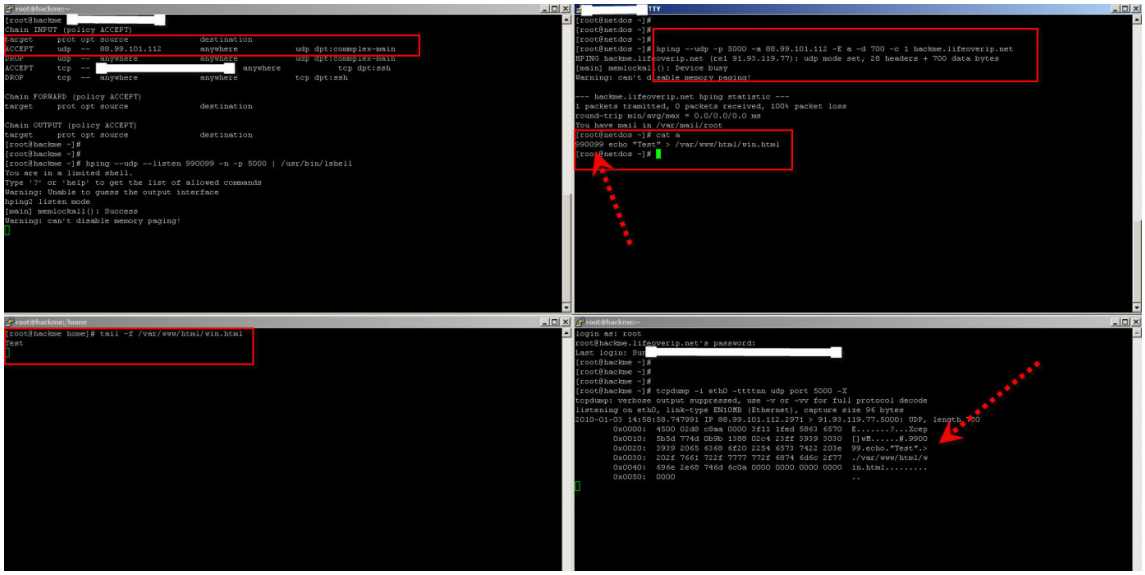
Bir sonraki adım 91.93.119.77 ip adresinin 5000. Portunda dinlemede olan bir shell'e IP spoofing yaparak komut gönderme ve takım ismini /var/www/html/win.html dosyasına yazdırmaktan ibaretti. Bu adımdaki engeller(bu adıma gelen takımlara ipucu olarak verilmiştir)

Gönderilen komutların başında 990099 eklemek gerekmektedir(990099 her onune gelenin uzaktan komut çalıştıramaması için basit bir önlem) ve 5000. Porta sadece 88.99.101.112(ip spoofing yapılması gerekecekti) ip adresinden bağlantı yapılabilmektedir.

Burada beklenen klasik hata portun TCP/UDP ne olduğunu belirlemeden TCP üzerinden IP spoofing yaparak porta veri gönderilmeye çalışılmasıydı. Portun TCP mi UDP mi olduğu 100 puanlık bir ipucu olduğu için hiçbir takım ipucu almadı. Bu adımı aşmak için nemesis, Scapy ya da hping gibi bir arac kullanarak spoof edilmiş UDP paketleriyle hedef sisteme komut gönderilmesi gerekiyordu.

 # nemesis udp -y 5000 -P komut.txt -S 88.99.101.112 -D hackme.lifeoverip.net

Komut.txt dosyasının içerisinde gönderilecek komut ve başında 990099 yazmalı.



Sonuç olarak yorucu ama güzel bir yarışma geçirdik. Çok şey öğrendik(ekiplerden biri public etmediği bir 0 day kullandi, başka bir ekip beklenmeyecek kadar kısa sürede sistemde root oldu, sistemler defalarca DDOS'a uğradı, kiminde ayağa kalktı kiminde kalkamadı).

Ekiplerden ikisinin hızlı davranması ve bunların artıklarını kullanıp sistem üzerinde oynamalar yapmak isteyen arkadaşlar olduğu için yarışmayı erkenden kapamak zorunda kaldık. Bu tip bir yarışmayı ilk defa online ve herkese açık olarak gerçekleştirdiğimiz için çeşitli tecrübeler yaşadık ve ders aldık. Sonraki yarışmalarda daha sağlıklı oyunlar düzenlemek dileğiyle...