

CYGWIN KURULUMU ve KULLANIMI

Cygwin, Microsoft Windows işletim sistemi üzerinde çalışan, open source, bir UNIX simülatörüdür. Cygwin`in asıl amacı *nix türevi sistemlerde yer alan yazılımların Windows işletim sisteminde çalışmasını sağlamaktır.

Bu makalemizde; Windows işletim sistemi yüklü bir bilgisayara Cygwin kurulumuna ve basit unix komutları aracılığıyla Cygwin kullanımına değineceğiz.

NOT: Makale *nix için uygulama geliştiren yazılımcılardan ya da *nix kurmadan nimetlerinden faydalanmak isteyen kullanıcılardan ziyade penetration testerlara yönelik olacaktır.

CYGWIN KURULUMU

Cygwin simülatörünü, resmi sitesinden (www.cygwin.com) ücretsiz olarak indirdikten sonra aşağıdaki adımları izleyerek sisteminize kurabilirsiniz;

1. Cygwin simülatörüne ait kurulum dosyasını (setup.exe) çalıştırıyoruz ve ilk adımı "İleri" diyerek geçiyoruz.
2. "Install from Internet" seçeneğini işaretleyerek bir sonraki adıma geçiyoruz.
3. Bu adımda Cygwin`in kurulacağı dizini belirleyip, sistemdeki tüm kullanıcıların oturumuna mı yoksa sadece sizin oturumuza mı kurulacağına karar verdikten sonra metin dosya tipini (binary/text) seçerek bir sonraki adıma geçiyoruz.
4. Bu adımda da paketlerin (packages) indirileceği/bulunacağı dizini seçip ilerliyoruz.
5. İnternet bağlantı seçeneklerinden isteğimize göre bir seçeneği işaretleyerek install işlemine başlamak için sonraki adıma geçiş yapıyoruz.
6. Dosyaların yükleneceği depoları seçerek kurulum işlemine başlamış oluyoruz.
7. "Select Packages" adımında gerekli olan paketleri seçip ilerliyoruz. (Not: Penetration Test için gerekli olabilecek paketleri seçmeniz yeterlidir. Örneğin; C exploitleri derlemek için gcc compiler paketlerini seçebilirsiniz)
8. İlgili paketleri seçtikten sonra ilerliyoruz ve download/install işleminin bitmesini bekliyoruz.
9. Kurulum işlemi bittikten sonra devamlı kullanacaksanız "Create icon on Desktop" seçeneğiyle masaüstüne kısa yol oluşturabilirsiniz.

Yukarıdaki aşamalarla kurulum işlemi sorunsuz bitiriyoruz..

CYGWIN KULLANIMI

Cygwin`i kurulum yaptığınız dizinden yahut masaüstündeki ya da başlat menüsündeki kısa yolundan çalıştırabilirsiniz.

Penetration test esnasında kullanacağınız exploits, wireless cracking tools, sniffers, network monitoring applications vb. gibi uygulamalarınıza ait dosyalarınızı isterseniz wget komutu ile çekebilir, isterseniz de harici olarak bilgisayarınızda Cygwin`in kurulu olduğu klasöre kopyalayabilirsiniz.

Not: “wget, ls, clear” vb. gibi basit unix komutlarına ihtiyaç duyabileceğiniz için makalenin son kısmında komutlara ait bilgiler verilecektir.

Perl Exploitlerinin Çalıştırılması

Bu örneğimizde Perl exploitlerinin nasıl çalıştırılacağını ve hedef sisteme nasıl uygulanacağını göreceğiz.

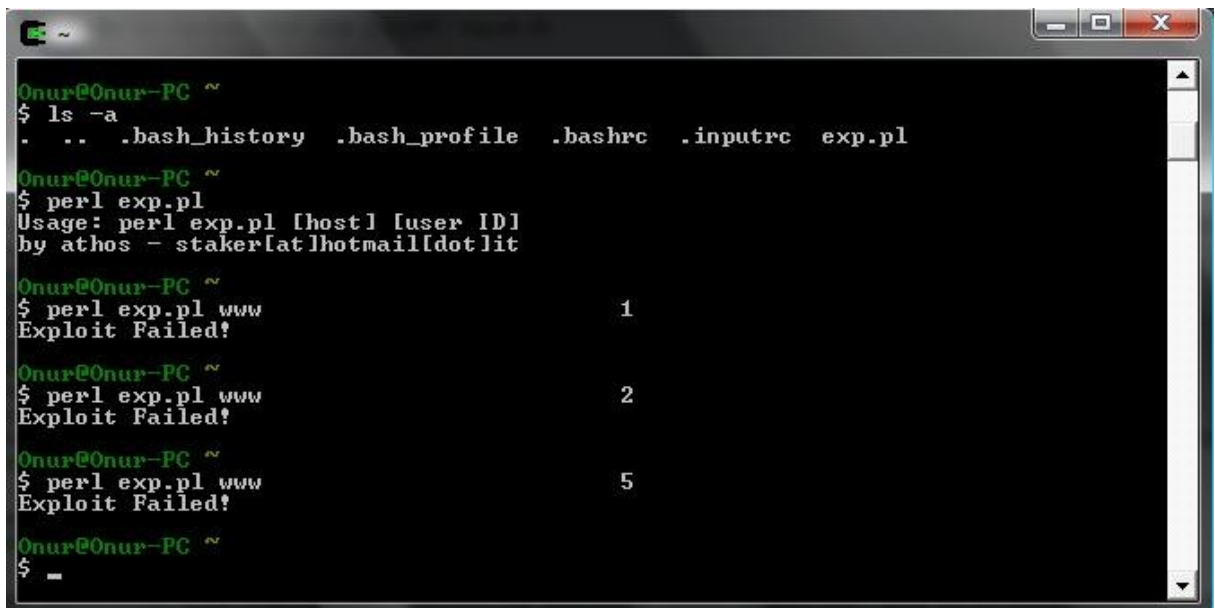
Exploitimizi wget komutu yardımıyla ya da haricen Cygwin`in kurulu olduğu klasöre attıktan sonra Cygwin ekranında “ls” komutu ile exploitimizi görebiliriz.

Exploitimizin perl ile yazıldığını öğrendiğimize göre, çalıştırmak için; “perl <file name>” komutunu veriyoruz. (Not: Perl Compiler paketinin kurulu olması gerekmektedir.)

İlgili komutu yazdıktan sonra exploitimiz çalışıyor ve ekrana bir çıktı veriyor. Bu çıktıdaki bilgiler aracılığıyla exploitimizin nasıl kullanılacağını (usage) öğreniyoruz.

Usage kısmında belirtilen söz dizimine uygun şekilde komutumuzu yazarak, exploitimizi çalıştırıyor ve hedef sistemi exploitlemiş oluyoruz.

Uygun exploitin seçilmesi, sistemde kurulu scriptin fixlenmemesi vb. gibi durumlara göre exploitimizin başarılı ya da başarısız olduğunu şekildeki gibi görebiliyoruz.



```
Onur@Onur-PC ~  
$ ls -a  
. .. .bash_history .bash_profile .bashrc .inputrc exp.pl  
Onur@Onur-PC ~  
$ perl exp.pl  
Usage: perl exp.pl [host] [user ID]  
by athos - staker[at]hotmail[dot]lit  
Onur@Onur-PC ~  
$ perl exp.pl www 1  
Exploit Failed!  
Onur@Onur-PC ~  
$ perl exp.pl www 2  
Exploit Failed!  
Onur@Onur-PC ~  
$ perl exp.pl www 5  
Exploit Failed!  
Onur@Onur-PC ~  
$ -  
$
```

Görüldüğü gibi Cygwin simülatörünün kurulumu ve kullanımını adım adım görerek, ne kadar basit olduğunu gözlemledik.

Şimdi de C ve Python ile yazılmış exploitlerin nasıl çalıştırılacağını görerek, bilgilerimizi pekiştirmeye çalışalım.

C Exploitlerini Derlemek

Perl exploitimizin nasıl çalıştırılacağını anlatırken, exploitimizi wget komutu ile çekerek ya da haricen Cygwin`in kurulu olduğu dizine attığımızı öğrenmiştik. Aynı şekilde C exploitimizi de edindikten sonra Cygwin`i açıyoruz.

Exploitimizin ilgili dizinde olup olmadığını kontrol etmek için, dizin içerisindeki dosyaları ls -a komutu ile listeliyoruz.

Exploitimizin C ile yazıldığından ötürü derlemek için gcc compilerini kullanacağız. "gcc -o filename filename.c" şeklinde komutumuzu yazıyoruz.

Komutumuzu çalıştırdıktan sonra gcc compiler herhangi bir hata uyarısı vermezse, kodumuz derlenmiş, .exe çıktısı hazırlanmış ve kullanıma hazır demektir. İşlemin başarılı olduğunu test etmek amacıyla tekrar "ls -a" komutunu vererek, exploitimize ait .exe dosyasının oluşturulup oluşturulmadığını kontrol ediyoruz.

.exe dosyamız oluşturulduğuna göre, artık exploitimizi çalıştırabilir ve kullanımı hakkında bilgi edinebiliriz. Exploitimizi çalıştırmak için "./filename" komutunu veriyoruz.

Komutumuzu çalıştırdığımızda exploitimiz ile bilgilere ve hedef sistemin nasıl exploit edileceğine dair kullanım bilgilerini görüyoruz ve ilgili söz dizimine uygun olarak exploitimizi çalıştırıyoruz, sonucu gözlemliyoruz.

```
Onur@Onur-PC ~
$ ls -a
.  ..  .bash_history  .bash_profile  .bashrc  .inputrc  exp.pl  webdav.c

Onur@Onur-PC ~
$ gcc -o webdav webdav.c

Onur@Onur-PC ~
$ ls -a
.  .bash_history  .bashrc  exp.pl  webdav.exe
.. .bash_profile  .inputrc  webdav.c

Onur@Onur-PC ~
$ ./webdav
IIS 5.0 WebDAV Exploit by RoMaNSoFt <roman@rs-labs.com>. 23/03/2003
Usage: ./webdav <target host> [target port] [bind port] [ret]
E.g 1: ./webdav victim.com
E.g 2: ./webdav victim.com 80 31337 0x4804

Onur@Onur-PC ~
$ ./webdav
[*] Resolving hostname ...
[*] Attacking port 80 at (EIP = 0x00480004)...
[*] Now open another console/shell and try to connect (telnet) to victim port 31337...
[*] Victim server issued the following 163 bytes of response:
---
HTTP/1.1 400 Bad Request
Content-Type: text/html
Date: Thu, 04 Dec 2008 13:55:23 GMT
Connection: close
Content-Length: 34

<h1>Bad Request <Invalid URL></h1>
---
[*] Server NOT vulnerable!
```

Python Exploitlerini Çalıştırmak

Python ile yazılmış exploitimizi Cygwin'in kurulu olduğu dizine aldıktan sonra, "python <filename.py>" komutu yardımıyla çalıştırıyoruz ve exploit ile ilgili kullanım bilgilerine ulaşıyoruz.

Kullanım bilgilerine uygun söz dizimi aracılığıyla komutumuzu yazarak, hedef sistemi exploit etmeye çalışıyoruz ve sonucu gözlemliyoruz.

```
Onur@Onur-PC ~
$ ls -a
.  .bash_history  .bashrc  disconn.py  mail.py  webdav.c
.. .bash_profile  .inputrc  exp.pl      rfpoison.py  webdav.exe

Onur@Onur-PC ~
$ python mail.py
usage : mail.py [target]

Onur@Onur-PC ~
$ python mail.py
usage : mail.py [target]

Onur@Onur-PC ~
$ python disconn.py
Traceback (most recent call last):
  File "disconn.py", line 31, in <module>
    import btk
ImportError: No module named btk

Onur@Onur-PC ~
$ python rfpoison.py
Sending poison...
Traceback (most recent call last):
```

Görüldüğü gibi exploitlerimize “python <filename.py>” komutunu verdiğimizde exploit ile ilgili bilgilere ulaşabiliyor, çalıştıktan sonra da olumlu ya da olumsuz sonuç alındığına dair bilgilendiriliyoruz.

Cygwin Avantajları ve Dikkat Edilmesi Gereken Noktalar

Cygwin makalemize giriş yaparken, Unix uygulamalarını Windows ortamında çalıştırmaya yarayan bir simülatör olduğuna değinmiştik. Buna istinaden; Cygwin kurulumu esnasında, Cygwin`i hangi amaçla kullanacaksanız (development, penetration testing etc.) yüklenmesini istediğiniz paketleri amacınıza uygun seçmeniz gerekmektedir.

Paketleri seçip kurulumu yaptıktan sonra amacınıza uygun olarak Windows ortamında Unix`in nimetlerinden faydalanmaya başlayabilir ve birçok ihtiyacınızı giderebilirsiniz.

Ayrıca Cygwin`e online olarak ulaşabilir ve internet bağlantısı olan her yerde ekstra paketler yükleyebileceğiniz için, erişim ve kullanım kolaylığı bakımından tercih edilmektedir.

Makalemizin sonuna geldik. Aşağıdan sık kullanılan bazı Unix komutlarını görebilirsiniz. Hepinize güvenli günler :)

Sık Kullanılan Unix Komutları

ls	Çalışma anındaki dosya ve dizinleri listeler (kısa)
ls -l	Çalışma anındaki dosya ve dizinleri listeler (uzun)
ls -al	Çalışma anındaki dosya ve dizinleri listeler (uzun .)
cd xyz	xyz dizinine geçer
cd ..	Bir üst dizine çıkar
cd	Ana dizine geçer
cd /usr/bin	/usr/bin dizinine geçer
pwd	Çalışma anındaki dizini gösterir(print working directory)
mkdir xyz	xyz adlı bir dizin oluşturur
rmdir xyz	xyz adlı dizini siler
rm -r xyz	xyz adlı dizini ve altdizinlerini siler