

Infinitum Academy

İçindekiler

1.1 Hping3 Kullanım Kılavuzu: Genel Kurs Bilgisi:

1.1.1 Infinitum Academy Kurs Materyalleri

1.1.2 Infinitum Academy Canlı Destek

1.1.3 Infinitum Academy Test Ortamı Erişimleri

1.2 Kurs Yaklaşımı için Genel Stratejiler

1.2.1 Kurs Materyalleri

1.2.2 Kurs Egzersizleri

1.3 Destek Sistemi

2.1 Hping3 Nedir?

2.1.1 Port Port Tarama ve Host Keşif Çeşitleri Nelerdir?

2.2 Hping3 Çalışmaları

2.2.1 Hping3 Kullanarak Ping Atmak

2.2.2 Hping3 Modları

Infinitum Academy

1.1 Hping3 Kullanım Kılavuzu: Genel Kurs Bilgileri

Hping3 ile güvenlik denetimi (pentest) (Infinitum Academy) kursuna hoş geldiniz!

Bu kurs, penetrasyon testleri ve Hping3 kullanımı hakkında bilgi sahibi olmak isteyen, Sistem ve Ağ Yöneticileri ile güvenlik uzmanları için oluşturulmuştur. Bu kurs, ağlara karşı kötü niyetli varlıklar tarafından kullanılan saldırıları ve teknikleri daha iyi anlamınıza yardımcı olacaktır.

Bu kursumuzda cevaplamak istediğimiz bazı sorular;

- Hping3 nedir?
- Hping3'te kullanabileceğimiz fonksiyonlar nelerdir?
- Ağ tarama çeşitleri nelerdir?

1.1.1 Infinitum Academy Kurs Materyalleri

Kurs, çevrimiçi kitap modüllerini ve eşlik eden kurs videolarını içerir. Kitap modüllerinde ve videolarda ele alınan bilgiler örtüşmektedir, yani kitap modüllerini okuyabilir ve ardından videoları izleyerek herhangi bir boşluğu doldurabilirsiniz veya tersini yapabilirsiniz. Bazı durumlarda, kitap modülleri videolardan daha detaylıdır. Diğer durumlarda, videolar kitap modüllerindeki bazı bilgileri daha iyi iletebilir. Her ikisine de dikkatlice dikkat etmeniz önemlidir. Kitap modülleri ayrıca çeşitli egzersizler içerir.

1.1.2 Infinitum Academy Canlı Deste

Infinitum Academy Kütüphanesi'nin sağ üst köşesindeki "Discord'a Bağlan" düğmesine tıklayarak erişilebilir. Canlı Destek, öğrenci yöneticilerimizle doğrudan iletişim kurmanıza olanak tanır.

Öğrenci yöneticileri, teknik konularda yardımcı olmak için mevcuttur, ancak kurs materyalleri ve egzersizlerdeki maddeleri de açıklığa kavuşturabilirler. Ayrıca, bir lab makinesinde tamamen takılı kaldıysanız ve elinizden gelenin en iyisini yaptıysanız, Öğrenci Yöneticileri yolunuza yardımcı olacak küçük bir ipucu verebilirler.

1.1.3 Infinitum Academy Test Ortamı Eriřimleri

Bu kısım ilgili lab'ler eklendikten sonra güncellenecektir.

1.2 Kurs Yaklaşımı için Genel Stratejiler

Her öğrenci benzersizdir, bu nedenle kursa ve materyallere yaklaşmak için mutlak en iyi yol yoktur. Kendi rahat hızınızda kursu tamamlamanızı teşvik etmek istiyoruz. Kendinizi takip etmek için zaman yönetimi becerilerini uygulamanız da gerekecektir.

Aşağıdaki yaklaşımı kurs materyallerine genel bir yaklaşım olarak öneriyoruz:

- Kayıt işlemi sonrasında sağlanan kaynaklarda bulunan tüm bilgileri inceleyin
- Kurs materyallerini inceleyin.
- Tüm kurs egzersizlerini tamamlayın.

1.2.1 Kurs Materyalleri

Yukarıdaki bilgileri inceledikten sonra, kurs materyallerine atlayabilirsiniz. Ders videoları ile başlamayı tercih edebilirsiniz ve sonra kitap modülleri içinde verilen o konu hakkındaki bilgileri gözden geçirebilirsiniz veya tam tersi, tercih ettiğiniz öğrenme tarzına bağlı olarak. Kurs materyallerini ilerlerken, konuları tam olarak anlamak için bazı modülleri tekrar izlemeniz veya okumanız gerekebilir.

Kursu bir maraton olarak ve bir sprint olarak değil ele almanızı öneririz. Zor kavramlarla daha fazla zaman geçirmekten çekinmeyin ve ardından kursa devam etmeden önce tam olarak anladığınızdan emin olun.

1.2.2 Kurs Egzersizleri

Bir sonraki modüle geçmeden önce, her modülün sonundaki egzersizleri tamamlamanızı öneririz. Bu, materyali anlamınızı test edecek ve ilerlemeye olan güveninizi artıracaktır.

Bu egzersizleri tamamlamak için gereken zaman ve çaba, mevcut beceri setinize bağlı olarak değişebilir. Bazı egzersizler zor olabilir ve önemli bir zaman alabilir. Özellikle daha zor egzersizlerde ısrarcı olmanızı teşvik etmek istiyoruz. Bu egzersizler, Infinitum Security Operations "Ne kadar uykusuz kalmak o kadar bilgi zenginliği " zihniyetinin geliştirilmesinde özellikle faydalıdır.

1.3 Destek Sistemi

Infinitum Hping3 KK, sabit bir tempolu bir kurs deęildir. Bu, zorlandığınız konular için ekstra zaman harcayarak kendi hızınızda ilerleyebileceğiniz anlamına gelir. Bu kursun hızından yararlanın ve yeni ve zor bir konu veya yöntemle uğraşmak için biraz daha fazla zaman harcamaktan çekinmeyin. Kendinizce bir şeyler keşfetmenin hiçbir duygusu yoktur!

Ayrıca, konuyla ilgili daha derinlemesine araştırma yaparak kendinizin de öğrenme yolculuğunu sürdürdüğünüzü umuyoruz.

Sorularınızın bir kısmının cevabını alma olasılığınızın yüksek olduğu Help Center'mıza (yardım merkezi) bakmanızı öneririz.

- <https://academy.infinitumsecops.com/destek/>

İhtiyacınız olan yardımı bulamazsanız, destek sayfasındaki Canlı Destek veya e-posta (academy@infinitumsecops.com) aracılığıyla Öğrenci Yöneticilerimizle iletişime geçebilirsiniz.

2.1 Hping3 Nedir?

Hping3, ağ güvenlik denetimlerinde kullanılan, TCP/IP protokolü için açık kaynaklı bir paket oluşturu ve çözümleyicidir. DOS saldırısı, Nmap taraması gibi fonksiyonları bulunan ve ağ üzerinden hedef sisteme çeşitli paketler göndererek bilgi toplamanıza yarayan Linux araçlarından (tool) biridir. Klasik “ping” uygulamasının daha işlevsel versiyonu olarak da düşünülebilir. Linux'a direk yüklü olarak geldiği için herhangi bir kurulumla ihtiyaç yoktur. Bu tool'u kullanarak yapacağımız bir port taramasında elde edebileceğimiz router(yönlendirici), firewall(güvenlik duvarı), sistem durumu ve sistem bilgileri gibi veriler biz hackerlar için oldukça önemli bir yer tutmaktadır.

Hping3 dışında kullanabileceğiniz diğer ağ keşif araçları;

- Nmap
- Nesus
- Wireshark
- OpenSSH
- Metasploit

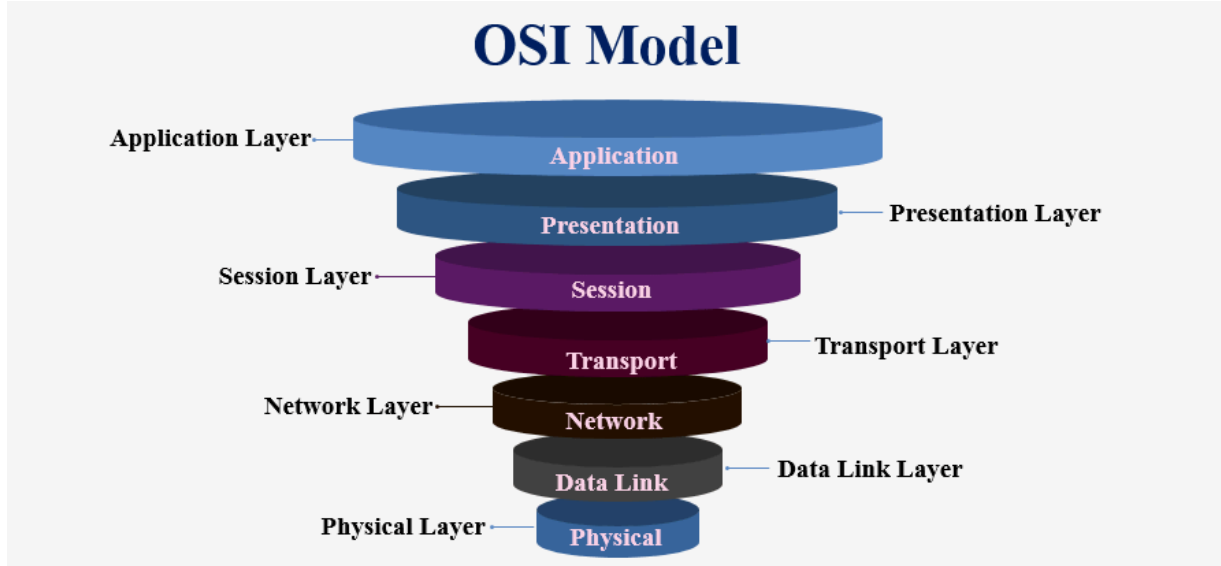
örnek olarak verilebilir.

2.1.1 Port Tarama ve Host Keşif Çeşitleri Nelerdir?

Port çeşitlerine girmeden önce port kavramını bir gözden geçirelim.Cihazlar arasındaki iletişimi sağlayan başlangıç ve bitiş noktaları arasındaki sanal köprüye port adı verilir. Yani cihazların network ağı içerisinde haberleşmesini sağlayan teknolojiye port denir.

Hping3 aracının TCP/IP protokolünü kullandığını söylemiştik. Peki TCP/IP nedir? Protokol nedir? Kısaca bir göz atalım.

Protokol: Günümüzdeki neredeyse her elektronik cihaz birbiriyle veri alışverişi durumundadır. Bu veri alışverişi gerçekleşirken veri alma ve iletme birimleri arasındaki organizasyonu sağlayan kurallara protokol adı verilir.



Şekil 1 OSI Referans Modeli

TCP(Transmission Control Protocol):İnternet iletişim kuralları dizisinin yani OSI Referans Modelinin 4.katmanı olan Ulaşım katmanına ait bir protokoldür. Cihazlar arasında paket alış-verişi sırasında paketleri şifreleyerek ve veri kaybını önleyerek ulaştırılmasını sağlayan protokole denir.

IP(Internet Protocol Address):Network içerisinde bulunan cihazlar veri paylaşımında bulunurken bu protokol sayesinde veriler yönlendirilir. OSI Referans Modelinin 3. Katmanı olan Ağ katmanına ait bir protokoldür.

TCP/IP:TCP ve IP protokollerinin birleşmesiyle oluşan ve cihazlar arasındaki data iletişiminin kurallarını belirleyen protokoller topluluğudur.

Şimdi de veri iletimi sırasındaki paket türüne göre çeşitlilik gösteren port tarama türlerine bir göz atalım.

- TCP Connect() Scan
- TCP ACK Scan
- TCP XMAS Scan
- TCP Window Scan
- IP Protocol Scan
- TCP SYN Scan
- TCP FIN Scan
- TCP NULL Scan
- UDP Scan
- Version detection(Sürüm belirleme)

- 1- TCP Connect() Scan: Tam bir bağlantı kurup ardından bağlantı kesilerek her bağlantı noktasına önemli sayıda paket gönderilmesini içerir. Diğer tarama türleriyle karşılaştırıldığında yavaştır.
- 2- TCP SYN Scan: Sadece üçlü el sıkışma olarak da adlandırılan SYN/ACK işleminin ilk aşaması olan SYN işlemini gerçekleştirdiği için TCP bağlantısını tamamıyla kurmaz ve bu sayede güvenlik duvarları tarafından da kısıtlanmayan bir tarama çeşididir. Bu yüzden yarı açık tarama olarak da adlandırılır ve açık, filtrelenmiş, kapalı port durumlarını gösterebilir. Hızlı ve verimli bir taramadır.

- 3- TCP ACK Scan: Sadece üçlü el sıkışma işleminin son aşaması olan ACK işlemini gerçekleştirdiği için TCP SYN Scan gibi bu tarama çeşidi de güvenlik duvarları tarafından kısıtlanmayan bir tarama çeşididir. Yine SYN taraması gibi bir bağlantı noktasının filtreleneip filtrelenmediğini belirlemeye yarar. Hızlı ve verimli bir taramadır.
- 4- TCP FIN(Stealth) Scan: Hedef makineye TCP bağlantı isteği kullanmadan gönderilen segmentle tarama yapılır. Tamamlandı anlamına gelen FIN bayrağı gönderenden daha fazla veri olmadığı anlamına gelir. Bu nedenle, göndericiden gönderilen son pakette kullanılır. Kaynak makinenin göndereceği FIN bayraklı segment, hedef makinenin kapalı bir portuna gelirse hedef makine RST + ACK bayraklı segment döndürecek, açık bir portuna gelirse bir tepki dönmeyecektir.
- 5- TCP XMAS Scan: TCP FIN Scan'den farklı olarak URG ve PSH bayraklarını kullanır. Aynı şekilde portların filtreleneip filtrelenmediğini belirlemeye yarar.
- 6- TCP NULL Scan: Diğer tarama türlerinden farklı olarak bayrak kullanmayan segmentler ile portların filtreleneip filtrelenmediğini belirlemeye yarar.
- 7- TCP Window Scan: TCP ACK Scan ile aynı olup tek farkı bir portun filtresiz olduğunu belirtmek yerine "open" ifadesini kullanır.
- 8- UDP Scan: TCP taramalarıyla aynı işlevi görür. Yani portların filtrelenmiş mi filtrelenmemiş mi olduğunu bizlere gösterir. Tek farkı UDP protokolünü kullanmasıdır.
- 9- IP Protocol Scan: Bir sunucunun ya da bir cihazın açık bağlantı noktasına sahip olup olmadığını tespit etmemizi sağlayan taramaya denir.
- 10- Version Detection: Bir cihazın sürümünü belirlemek, kullandığı hizmet ve uygulama sürümlerini elde etmek için kullanılan tarama türüdür.

Port türlerine göz attığımıza göre şimdi de Host keşif çeşitlerine bakalım.

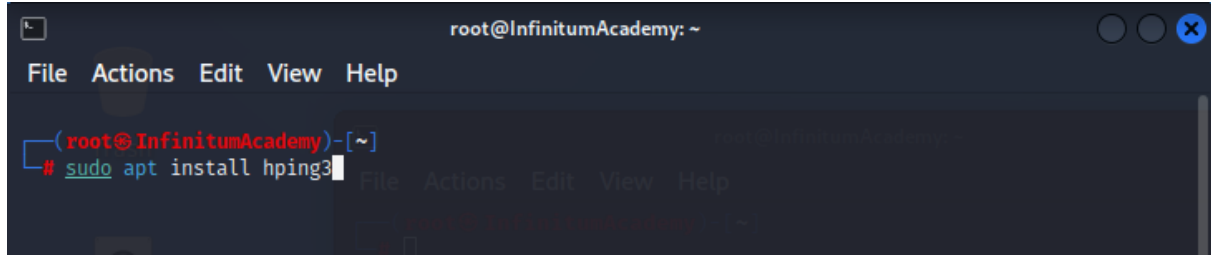
- Ping
- TCP Ping
- UDPing
- Arping

Ping: Bir veri paketinin ilgili sunucuya iletilmesi sırasında geçen süredir. TCP Ping, UDPing, Arping TCP, UDP ve ARP protokollerini kullanan ping çeşitleridir.

2.2 Hping3 Çalışmaları

Çalışmalarımıza geçmeden önce Nmap gibi daha kapsamlı bir ağ denetim aracı varken neden Hping3 kullanırsınız sorusuna bir açıklık getirelim. Bazı Nmap taramaları taramayı tamamladıktan sonra birtakım sistemler otomatik olarak sorguyu kitlediği için Nmap taramalarından önce Hping3 ile tarama yapmak daha sağlıklı sonuç elde etmenizi sağlayacaktır.

Hping3 tool'unun hali hazırda sisteminizde yüklü olduğunu bahsetmiştik. Ama yine de yüklü değilse terminalinize gireceğiniz “\$ sudo apt install hping3” komutu ile kurulumu kolaylıkla sağlayabilirsiniz.



```
root@InfinitemAcademy: ~  
File Actions Edit View Help  
(root@InfinitemAcademy)-[~]  
# sudo apt install hping3
```

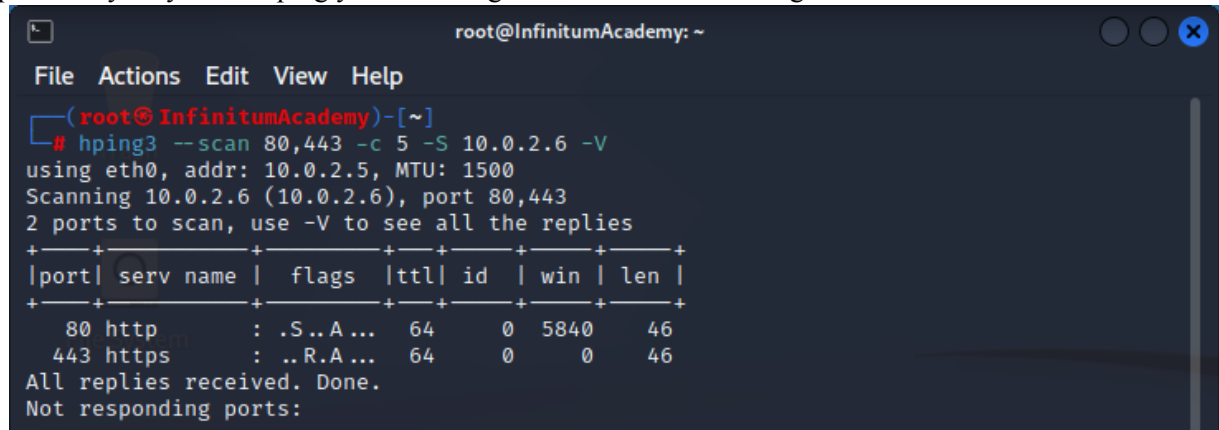
Şekil 2 Hping3 Aracını Terminal Üzerinde Yükleme

2.2.1 Hping3 Kullanarak Ping Atmak

Tool'umuuzu kullanarak yapacağımız ilk çalışmada herhangi bir IP adresine paket göndererek o IP adresinin çalışıp çalışmadığını anlamaya çalışacağız. Bu çalışmayı yapmak için yukarıda da anlatmış olduğumuz ping komutunu çalıştıracacağız. Ping komutu, çoğu sistemde ağa girişte ve çıkışta kısıtlanmış olan ICMP echo-request paketleri göndermektedir. Örneğin;



Bilgisayarımızdan hedef sisteme yolladığımız ping komutu firewall tarafından engellenecek ve herhangi bir sonuç elde edemeyeceğizdir. Bu yüzden ping komutundaki engellenen paketler yerine TCP ve UDP paketleri yollayan TCP ping ya da UDPing kullanmamız bize istediğimiz sonucu verecektir.



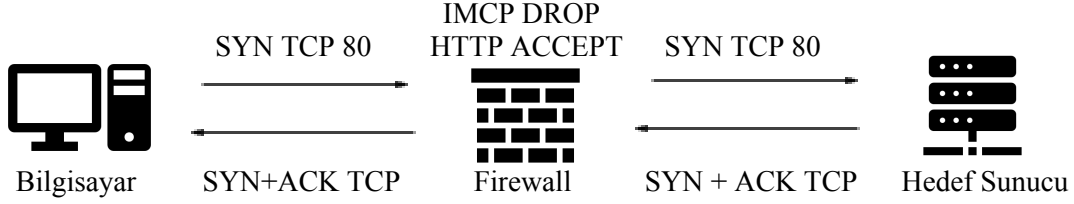
```
root@InfinitemAcademy: ~  
File Actions Edit View Help  
(root@InfinitemAcademy)-[~]  
# hping3 --scan 80,443 -c 5 -S 10.0.2.6 -V  
using eth0, addr: 10.0.2.5, MTU: 1500  
Scanning 10.0.2.6 (10.0.2.6), port 80,443  
2 ports to scan, use -V to see all the replies  
+-----+-----+-----+-----+-----+-----+  
|port| serv name | flags | ttl | id | win | len |  
+-----+-----+-----+-----+-----+-----+  
80 http : .S..A... 64 0 5840 46  
443 https : ..R.A... 64 0 0 46  
All replies received. Done.  
Not responding ports:
```

Şekil 3 TCP SYN Scan Örneği

Not: Örneklerimizde kullandığımız IP adresi zafiyetli bir sistem olan metasploitable II 'ye aittir.

Şekil 4'de bulunan komutu inceleyecek olursak komutumuzda tarama yapacağımız için “—scan” parametresini kullandık ve ardından tarama yapacağımız portları sırasıyla girdik. Ardından “-c” parametresini girerek kaç tane ping atılacağını belirtiyoruz. 5 tane ping atmak istediğimiz için “5” girdik. Sonra “-S” parametresini kullanarak “SYN” taraması yapacağımızı belirtiyoruz ve hemen ardından hedef sunucunun IP adresini giriyoruz. Komutumuzun sonuna “-V” parametresini girerek bize tüm portlar hakkında bilgi vermesini istiyoruz.

Bize verilen sonuçlara bakacak olursak 443 numaralı port'un "win" değeri 0 olarak görülmektedir. Bu port'un kapalı olduğu bilgisini bizlere vermektedir. 80 numaralı port'a bakacak olursak port'un açık olduğunu ve flag kısmındaki "S" ve "A" dönütlerinden yolladığımız paketlerin üçlü el sıkışma gerçekleştirerek başarılı bir şekilde ulaştığını görmüş oluyoruz. Şu anki durum;



Şeklinde ifade edilebilir. Görüldüğü üzere zafiyetli metasploitable II makinesinin 80 numaralı portunun açık olduğunu TCP SYN Scan sayesinde öğrenmiş bulunduk.

Bu işlem dışında direk "\$ sudo hping3 [IP Address]" komutunu kullanarak da TCP paketlerinin gönderilmesini sağlayabiliriz. Bizim Şekil 4'de yazmış olduğumuz koddan farklı olarak sürekli paket gönderme işlemi gerçekleştirecektir.

```
root@InfinitemAcademy: ~
File Actions Edit View Help

(root@InfinitemAcademy)-[~]
# sudo hping3 10.0.2.6
HPING 10.0.2.6 (eth0 10.0.2.6): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=10.0.2.6 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=9.6 ms
len=46 ip=10.0.2.6 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=7.0 ms
len=46 ip=10.0.2.6 ttl=64 DF id=0 sport=0 flags=RA seq=2 win=0 rtt=6.6 ms
len=46 ip=10.0.2.6 ttl=64 DF id=0 sport=0 flags=RA seq=3 win=0 rtt=5.8 ms
len=46 ip=10.0.2.6 ttl=64 DF id=0 sport=0 flags=RA seq=4 win=0 rtt=4.9 ms
len=46 ip=10.0.2.6 ttl=64 DF id=0 sport=0 flags=RA seq=5 win=0 rtt=3.0 ms
len=46 ip=10.0.2.6 ttl=64 DF id=0 sport=0 flags=RA seq=6 win=0 rtt=5.9 ms
^C
— 10.0.2.6 hping statistic —
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 3.0/6.1/9.6 ms
```

Şekil 4 Sürekli TCP Paketi Gönderme İşlemi

Şekil 5'deki "flag" ve "win" değerlerinden anlaşılacağı üzere portların kapalı olduğu bilgisine ulaşabiliriz.


```
root@InfinitemAcademy: ~  
File Actions Edit View Help  
  
(root@InfinitemAcademy)-[~]  
# hping3 --scan 75-85 -c 3 -S 10.0.2.6 -V  
using eth0, addr: 10.0.2.5, MTU: 1500  
Scanning 10.0.2.6 (10.0.2.6), port 75-85  
11 ports to scan, use -V to see all the replies  
+---+---+---+---+---+---+---+  
|port| serv name | flags | ttl | id | win | len |  
+---+---+---+---+---+---+---+  
75      : ..R.A... 64    0    0    46  
76      : ..R.A... 64    0    0    46  
77      : ..R.A... 64    0    0    46  
78      : ..R.A... 64    0    0    46  
79 finger : ..R.A... 64    0    0    46  
80 http   : .S..A... 64    0 5840    46  
81      : ..R.A... 64    0    0    46  
82      : ..R.A... 64    0    0    46  
83      : ..R.A... 64    0    0    46  
84      : ..R.A... 64    0    0    46  
85      : ..R.A... 64    0    0    46  
All replies received. Done.  
Not responding ports:
```

Şekil 5 Verilen Port Aralığında TCP SYN Scan Çıktısı

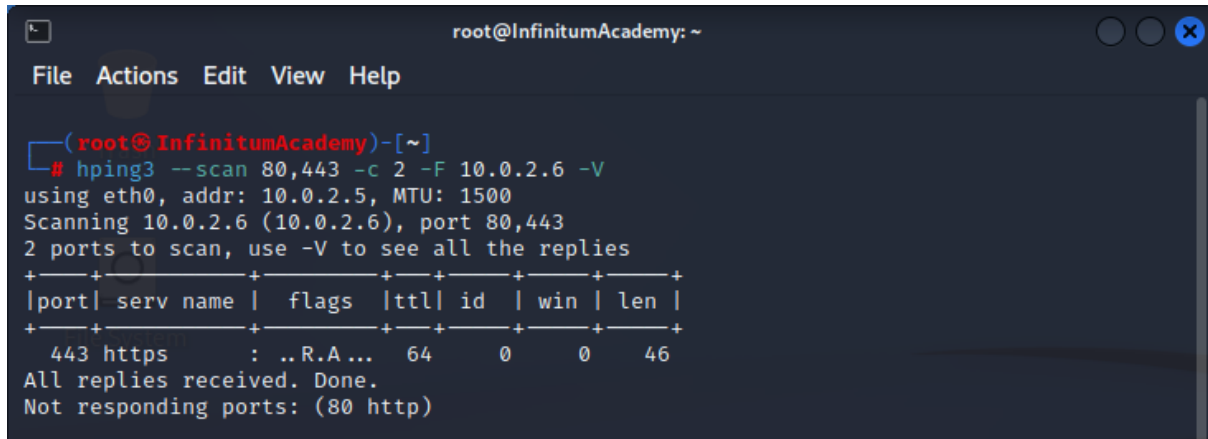
Şekil 6’da ise belirli bir port değeri yerine port aralığı belirleyerek TCP SYN Scan uygulamasının çıktısını görebilirsiniz. 80 numaralı port’un önceden de belirtmiş olduğumuz gibi açık olduğunu diğer diğer portların ise “R” ve “A” flag’lerini vermiş olduğunu yani kapalı olduğunu görebiliyoruz.

Biz örneklerimizde zafiyetli bir makine kullandığımız için kapalı portların “RA” flag’lerini verdiğini görüyoruz. Fakat herhangi bir sistem firewall ile korunuyor ya da host kapalı ise bize herhangi bir dönüt vermeyecektir.

```
root@InfinitemAcademy: ~  
File Actions Edit View Help  
  
(root@InfinitemAcademy)-[~]  
# hping3 --scan 79,80,81 -c 3 -S 10.0.2.6 -V  
using eth0, addr: 10.0.2.5, MTU: 1500  
Scanning 10.0.2.6 (10.0.2.6), port 79,80,81  
3 ports to scan, use -V to see all the replies  
+---+---+---+---+---+---+---+  
|port| serv name | flags | ttl | id | win | len |  
+---+---+---+---+---+---+---+  
^C  
  
(root@InfinitemAcademy)-[~]  
#
```

Şekil 6 Firewall Koruması Bulunan ya da Host'un Kapalı Olma Durumundaki Çıktı

Şekil 7’de görüldüğü üzere herhangi bir port taraması zafiyetli makine kapalı olduğu için gerçekleştirilememektedir. Döngüden çıkmak için “Ctrl+C” tuşlarıyla çıkış sağlayabilirsiniz.

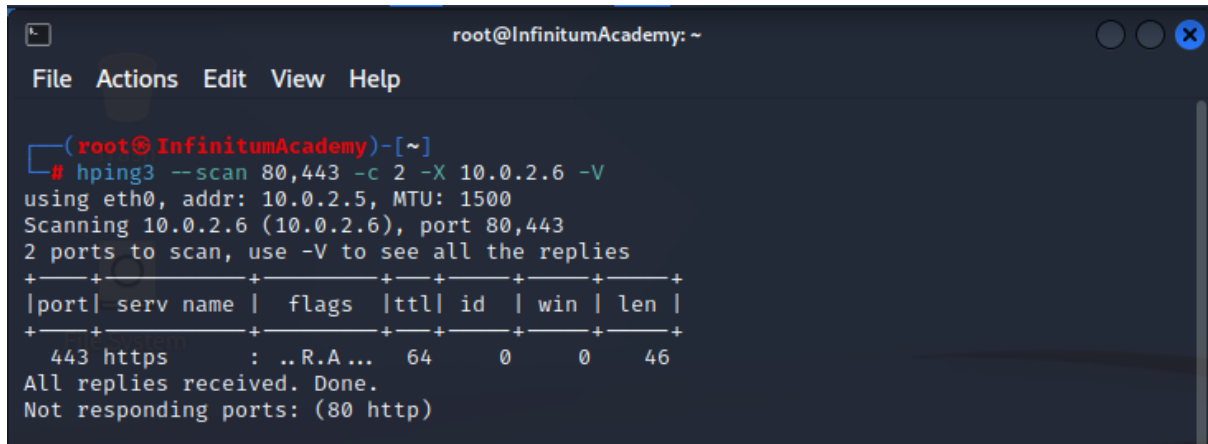


```
root@InfinitumAcademy: ~  
File Actions Edit View Help  
  
(root@InfinitumAcademy)-[~]  
# hping3 --scan 80,443 -c 2 -F 10.0.2.6 -V  
using eth0, addr: 10.0.2.5, MTU: 1500  
Scanning 10.0.2.6 (10.0.2.6), port 80,443  
2 ports to scan, use -V to see all the replies  
+-----+-----+-----+-----+-----+-----+  
|port| serv name | flags | ttl | id | win | len |  
+-----+-----+-----+-----+-----+-----+  
443 https   : ..R.A... 64    0    0   46  
All replies received. Done.  
Not responding ports: (80 http)
```

Şekil 7 TCP FIN Scan Çıktısı

Şekil 8’de farklı bir tarama çeşidi olan TCP FIN taramasının sonucunu görmekteyiz. Görüldüğü üzere FIN taraması sonucunda 80 port’u ile ilgili bilgi bulunmazken 443 numaralı port’ta “RA” flag’lerine rastlamaktayız. Bunun nedeni FIN Scan yaptıktan sonra port açık ya da firewall korumasından geçemeyen port’ların bizlere “Not responding ports: (80 http)” şeklinde belirtilirken, kapalı port’lar “RA” flag’leriyle belirtilir.

Bunların dışında yazdığınız komuta “-E” parametresi ekledikten sonra eklemek istediğiniz dosyanın ismini, dosyanın türünü belirterek, girerseniz dosya transferi gerçekleştirebilirsiniz.



```
root@InfinitumAcademy: ~  
File Actions Edit View Help  
  
(root@InfinitumAcademy)-[~]  
# hping3 --scan 80,443 -c 2 -X 10.0.2.6 -V  
using eth0, addr: 10.0.2.5, MTU: 1500  
Scanning 10.0.2.6 (10.0.2.6), port 80,443  
2 ports to scan, use -V to see all the replies  
+-----+-----+-----+-----+-----+-----+  
|port| serv name | flags | ttl | id | win | len |  
+-----+-----+-----+-----+-----+-----+  
443 https   : ..R.A... 64    0    0   46  
All replies received. Done.  
Not responding ports: (80 http)
```

Şekil 8 XMAS Scan Çıktısı

Şekil 8’de ise XMAS taraması sonuçlarını görmekteyiz. Bu tarama türü de TCP FIN Scan’de olduğu gibi kapalı port’larda “RST/ACK” yani “RA” çıktısı verirken ,açık portlar aynı FIN taramasındaki gibi çıktı vermeyecektir.

```
root@InfinitemAcademy: ~  
File Actions Edit View Help  
root@InfinitemAcademy)-[~]  
# hping3 --tcp-timestamp 10.0.2.6 -p 80 -S -c 5  
HPING 10.0.2.6 (eth0 10.0.2.6): S set, 40 headers + 0 data bytes  
len=56 ip=10.0.2.6 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5792 rtt=3.4 ms  
TCP timestamp: tcpts=4294950419  
  
len=56 ip=10.0.2.6 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=5792 rtt=3.8 ms  
TCP timestamp: tcpts=4294950519  
HZ seems hz=100  
System uptime seems: 497 days, 2 hours, 25 minutes, 5 seconds  
  
len=56 ip=10.0.2.6 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=5792 rtt=3.9 ms  
TCP timestamp: tcpts=4294950619  
HZ seems hz=100  
System uptime seems: 497 days, 2 hours, 25 minutes, 6 seconds  
  
len=56 ip=10.0.2.6 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=5792 rtt=7.9 ms  
TCP timestamp: tcpts=4294950720  
HZ seems hz=100  
System uptime seems: 497 days, 2 hours, 25 minutes, 7 seconds  
  
len=56 ip=10.0.2.6 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=5792 rtt=2.0 ms  
TCP timestamp: tcpts=4294950820  
HZ seems hz=100  
System uptime seems: 497 days, 2 hours, 25 minutes, 8 seconds  
  
— 10.0.2.6 hping statistic —  
5 packets transmitted, 5 packets received, 0% packet loss  
round-trip min/avg/max = 2.0/4.2/7.9 ms
```

Şekil 9 TCP Paketleri İle Timestamp Uygulaması

Yukarıda ise görüldüğü üzere TCP paketleri ile zafiyetli cihazımıza ait Timestamp uygulayarak uptime bilgilerini elde edebiliyoruz.

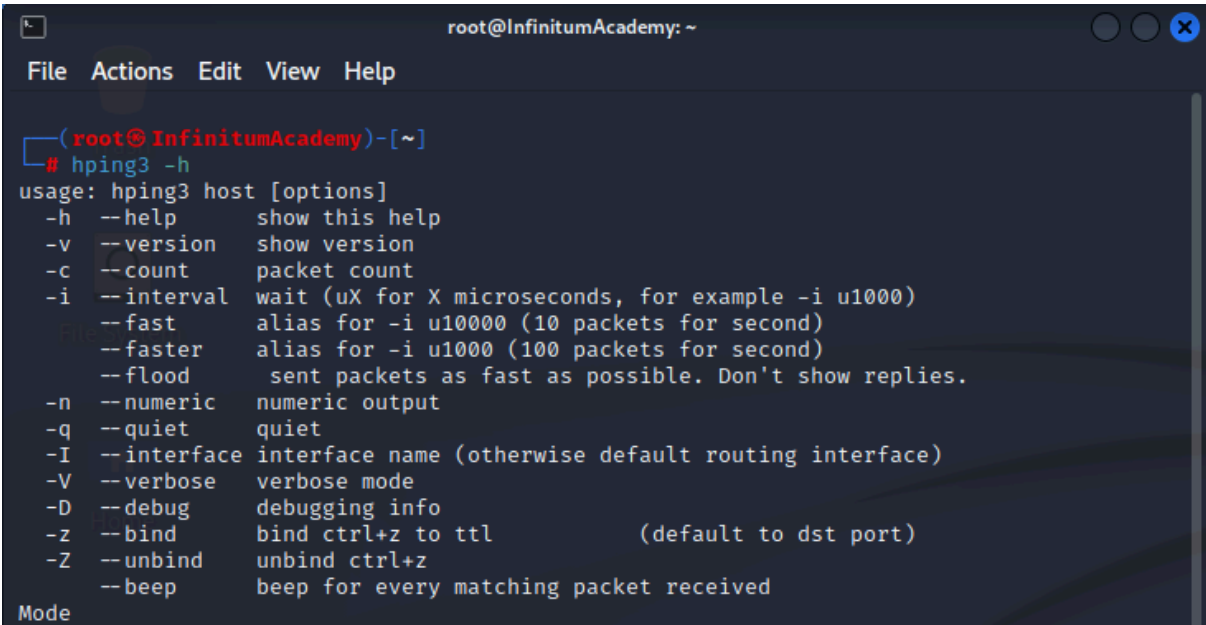
2.2.2 Hping3 Modları

Bildiğiniz üzere Hping3 tarama çeşitlerinden TCP'yi varsayılan olarak kullanmaktadır. Ama siz isterseniz mod değişikliğini belli parametreleri girerek sağlayabilirsiniz. Bu kodlar:

- -0 veya -rawip parametreleri RAW IP paketleri
- -1 veya -icmp parametreleri ICMP paketleri
- -2 veya -udp parametreleri UDP paketleri
- -8 veya -scan parametreleri varsayılan TCP paketleri
- -9 veya -listen parametreleri Dinleme Modu şeklindedir.

Hping3 komutlarının nasıl kullanıldığı ve komutların ne işe yaradığı hakkında daha detaylı bilgi edinmek

istiyorsanız terminalinizde “hping3 --help” ya da “hping3 -h” komutunu kullanarak erişebileceğiniz komutlar hakkında bilgi sahibi olabilirsiniz.

A terminal window titled 'root@InfinitumAcademy: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(root@InfinitumAcademy)-[~]'. The command '# hping3 -h' has been entered, resulting in the following output:

```
usage: hping3 host [options]
-h --help          show this help
-v --version       show version
-c --count         packet count
-i --interval      wait (uX for X microseconds, for example -i u1000)
                  --fast      alias for -i u10000 (10 packets for second)
                  --faster    alias for -i u1000 (100 packets for second)
                  --flood     sent packets as fast as possible. Don't show replies.
-n --numeric       numeric output
-q --quiet         quiet
-I --interface     interface name (otherwise default routing interface)
-V --verbose       verbose mode
-D --debug         debugging info
-z --bind          bind ctrl+z to ttl          (default to dst port)
-Z --unbind        unbind ctrl+z
--beep            beep for every matching packet received
```

The word 'Mode' is visible at the bottom left of the terminal window.

Şekil 10 Terminaldeki "hping --help" Komut Çıktısı