Sanal Sunucuları Nasıl Belirleyebiliriz

Deniz Çevik, Şubat 2010, WGT E-Dergi 4. Sayı

TCP Paket Başlığındaki Değerler

TTL (Time To Live) Alanı: Yollanan paketin kaç hop boyunca geçerli olacağını gösteren bir alandır. Aynı zamanda hedef sistemin bizden ne kadar uzakta olduğunu da belirtir. Her işletim sistemi bu değeri belirli bir rakamdan azaltır. Örneğin Windows tabanlı sistemlerde 128, Sun Solaris işletim sistelerinde 256 değeri başlangıç TTL değeridir. İşletim sistemini belirlemek içinde kullanılabilecek bu alan aynı sisteme ait olduğunu düşündüğünüz IP adresleri için mutlaka aynı olmalıdır.

MSS ve TCP WINDOW Size: Bu değerler aynı sistemden yollanan paketler için mutalaka aynı olmalıdır. Aynı ağda bulunan benzer işletim sistemlerinde söz konusu değerler aynı olabilir, bu sebeple söz konusu değerlerin aynı olması ayırt edici bir özellik olmasa da farklı olmaları durumunda paketlerin farklı fiziksel sistemden üretildiğini söylemek yanlış olmayacaktır.

IP (tos 0x0, ttl 127, id 3093, offset 0, flags [DF], proto TCP (6), length 88) 192.168.1.3.43140 > 10.0.0.1.80: P 481:529(48) ack 26208 win 16384

IPID Alanı: Farklı IP adreslerinin açık portuna gönderilen SYN paketine alınan cevaplardaki IPID değerlerinin birbirini takip edecek şekilde üretiliyor olmaları gerekmektedir. Tabi bu yöntem söz konusu alan ardışık olarak üretiliyor ise kullanışlı olacaktır. Eğer IPID değeri sabit 0 olarak üretiliyor veya rastgele değerlerden seçiliyor ise bu alana bakarak yorum yapmak mümkün olmayacaktır. Bununla birlikte TCP/IP altyapısına yönelik sıkılaştırma yapılmamış Windows tabanlı sistemlerde oldukça başarılı sonuçlar verebilir.

```
# hping -S -p 80 10.0.0.1
 HPING 10.0.0.1 (eth2 10.0.0.1): S set, 40 headers + 0 data bytes
 len=46 ip=10.0.0.1 ttl=126 id=25701 sport=80 flags=SA seq=0 win=16384 rtt=21.3 ms
 len=46 ip=10.0.0.1 ttl=126 id=25702 sport=80 flags=SA seq=1 win=16384 rtt=18.7 ms
 len=46 ip=10.0.0.1 ttl=126 id=25704 sport=80 flags=SA seq=2 win=16384 rtt=18.5 ms

# hping -S -p 80 10.0.0.2
 HPING 10.0.0.2 (eth2 10.0.0.2): S set, 40 headers + 0 data bytes
 len=46 ip=10.0.0.2 ttl=126 id=25705 sport=80 flags=SA seq=0 win=16384 rtt=21.3 ms
 len=46 ip=10.0.0.2 ttl=126 id=25707 sport=80 flags=SA seq=1 win=16384 rtt=18.7 ms
 len=46 ip=10.0.0.2 ttl=126 id=25711 sport=80 flags=SA seq=2 win=16384 rtt=18.5 ms

# hping -S -p 80 10.0.0.1
 HPING 10.0.0.1 (eth2 10.0.0.1): S set, 40 headers + 0 data bytes
 len=46 ip=10.0.0.1 ttl=126 id=25712 sport=80 flags=SA seq=0 win=16384 rtt=21.3 ms
 len=46 ip=10.0.0.1 ttl=126 id=25713 sport=80 flags=SA seq=1 win=16384 rtt=18.7 ms
 len=46 ip=10.0.0.1 ttl=126 id=25717 sport=80 flags=SA seq=2 win=16384 rtt=18.5 ms
```

TCP-Timestamp Değeri: Eğer hedef işletim sistemleri TCP-Timestamp isteklerine cevap veriyor ise farklı IP adreslerine yollanan cevapların aynı değeri üretmesi veya hesaplanan uptime sürelerinin aynı olması bize bu IP adreslerinin aynı sisteme atanmış sanal IP adresleri olduğu bilgisini verebilir. TCP-Timestamp değerlerini hping aracı ile görebiliriz.

```
# hping -S -p 80 10.0.0.5 --tcp-timestamp
HPING 10.0.0.5 (eth2 10.0.0.5): S set, 40 headers + 0 data bytes
len=56 ip=10.0.0.5 ttl=62 id=0 sport=80 flags=SA seq=0 win=5792 rtt=21.5 ms
 TCP timestamp: tcpts=203291022

len=56 ip=10.0.0.5 ttl=62 id=0 sport=80 flags=SA seq=1 win=5792 rtt=18.0 ms
 TCP timestamp: tcpts=203291271
 HZ seems hz=100
 System uptime seems: 23 days, 12 hours, 41 minutes, 52 seconds
```

TCP başlığında yer alan değerler bizlere kesin sonuçlar vermese de , paketlerin aynı sistemden üretilmiş olabileceğine dair ipucları sunmaktadır. Bununla birlikte HTTP cevap başlığındaki bazı değerler daha kesin yargılara ulaşmamıza yadımcı olabilir.

HTTP Cevap Başlığındaki Değerler

Date Başlığı: HTTP cevaplarında yer alan Date alanı, aynı sistemlerden üretilen cevaplarda aynı olacaktır.

```
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Accept-Ranges: bytes
ETag: "0c3110c9d9c21:2e6"
Server: Microsoft-IIS/6.0
Date: Wed, 20 Jan 2010 17:50:45 GMT
```

ETAG Başlığı: Microsoft IIS tabanlı sistemlerde aynı sunucu tarafından üretilen HTTP cevaplarındaki ETAG başlığının ikinci bölümü aynı olmalıdır.

```
ETag: "0c3110c9d9c21:2e6"
```

Content-Location Başlığı: Web sunucu yazılımı, yerel IP adresinin veya sunucu hostname bilgisinin Content-Location başlığında yayınlanmasına neden olan açıklardan etkileniyor ise her sistemde benzer sorunların bulunması veya aynı bilgilerin çıktılarda yer alması gerekecektir. Özellikle Microsoft IIS tabanlı web sunucular, Host başlığı bulunmayan HTTP/1.0 ile gelen istekler için ürettikler yönlendirme mesajlarında sunucunun yerel ağda kullanılan IP adresini Content-Location bölümüne ekleyebilirler. Yöneldirme mesajlarının oluşması için mevcut dizinlere / karakteri eklemeden istekte bulunmak yeterli olacaktır.

GET /css HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://10.0.0.3/iisstart.htm

Realm Başlığı: Basit yetkilendirme tanımlamaları için kullanılan REALM başlıklarında yer alan sunucu adı veya lokal ip adresi bilgilerinin aynı olması durumunda da benzer yargılara varılabilir.

HTTP/1.1 401 Unauthorized
Content-Length: 83
Content-Type: text/html
Server: Microsoft-IIS/6.0
WWW-Authenticate: Negotiate
WWW-Authenticate: NTLM
WWW-Authenticate: Basic realm="test.local"