ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/nmap-hping/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Hping%20&%20Nmap.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Açık kaynak kodlu araçlar birer “ürün” degildir. Birer projedir. Bu sebeple açık kaynak kodlu araçlar genelde piyasada bulunan muadil ürünlere nispeten teknik olarak aynı seviyeyi yakalamış olsa da kullanım kolaylığı, esneklik ve birinci elden ticari destek yönünden geride kalmışlardır. Bu da tüm sorumlulugun yazılımı kullanana ait olması zorunluluğunu beraberinde getirmektedir.

(Page 1)

2)

Hping

Hping istenilen türde TCP/IP paketi oluşturmak için kullanılan bir tool’dur. Oluşturulacak paketlerdeki tüm alanların kendimize özgü belirlenebilmesini sağlar. Hping çıktılarını yorumlamak için orta düzey TCP/IP bilgisi gereklidir. Hping’in klasik otomatize araçlardan – mesela Nmap’ten – farkı tamamen kendi oluşturduğumuz paketleri ağa gönderebilmemizdir. Bu yüzden Tcp/ip bilgisine ihtiyaç vardır. Mesela Nmap’te Xmas tarama paketleri -SX parametresi ile “otomatikmen” oluşturulurken hping’de Xmas tarama paketleri Xmas’a özgü TCP bayraklarından haberdar olan bir kimsenin ona göre hping parametrelerini kullanmasıyla oluşturulur.

(Page 4)

3)

Hping’le yapılabilecekler:

- Gelişmiş Port Tarama
- Gelişmiş traceroute
- İşletim Sistemi Saptama
- DDOS Testleri
- Hedef sistemin uptime süresini saptama

(Page 4-5)

4)

Hping Kullanım Örnekleri

a) Bilindiği üzere ping komutu ICMP paketi gönderir ve alır. Hping3 komutu ise --icmp parametresi verilmediği takdirde varsayılan olarak TCP paketi gönderir. O yüzden aşağıdaki komut hedefe TCP paketi gönderecektir.

> hping3 www.includekarabuk.com

Output:

HPING www.includekarabuk.com (eth0 93.89.224.247) : NO FLAGS are set, 40 headers + 0 data bytes

^C

----- www.includekarabuk.com hping statistic ----

19 packets transmitted, 0 packets received, %100 packet loss.

round-trip min/avg/max = 0.0/0.0/0.0 ms

b) Yukarıdaki kullanım ile hedef sistemin 0. portuna TCP paketi gönderilir. Farklı bir portuna paket gönderebilmek için -p parametresi kullanılmalıdır.

> hping3 www.includekarabuk.com -p 80

c) UDP paketi göndermek için --udp, ping paketi göndermek için --icmp, ip paketi göndermek için --rawip parametreleri kullanılır. Örn;

> hping3 www.includekarabuk.com --rawip

d) Oluşturulacak TCP paketinin bayrağını belirlemek için bayrağın isminin ilk harfini parametre olarak hping3 komutuna eklemek yeterlidir. Örn;

> hping3 www.includekarabuk.com -R // -R means flag RST.

Diğer popüler bayraklar; SYN (-S), ACK (-A), FIN (-F), URGENT (-U), TCP Sequence Number (-M),...

e) Hping3 ile port taraması yapmak için --scan parametresi kullanılır.

> hping3 www.karabuk.edu.tr --scan 21,53,80,443,110-115 -S // SYN Taraması

Output:

Port	serv name	ttl	win	len
80	http	113	9652	46

f) Hping3'e göndereceği paketlerin sayısını söyleyebilmekteyiz.

> hping3 -c 3 www.includekarabuk.com

5)

DDOS saldırılarında amaç farklı farklı kaynaklardan olabildiğince fazla paket hedefe göndererek hedefteki hattın, sistemin kapasitesinin dolmasını ve yeni bağlantıları kabul edememesini sağlamaktır. Bunun için genellikle büyük boyutlu UDP paketleri kullanılır. Fakat SYN Flood ile de aynı işlem gerçekleştirilebilir.

> hping3 -S --rand-source www.karabuk.edu.tr -p 80 -I eth0 --flood // I : interface

(Page 5-6)

6)

Hping3 ile IDS/IPS Sistemlerini Test Etme

Hping3 ile oluşturulan paketlere payload eklenebilmektedir. Bu şekilde sorumlu olunan ağda kullanılan IDS/IPS sistemleri test edilebilmektedir. Örneğin

GET /cgi-bins/scripts/slxweb.dll/view?../../../../../etc/passwd HTTP/1.0

verisini içeren bir dosyayı -E parametresini kullanarak hedefin 80.portuna hping3 ile gönderdiğimizde hedefin önündeki IDS/IPS sisteminin uyarı vermesi gerekir. Bu ve buna benzer çeşitli methodlarla IDS sistemleri test edilebilmektedir.

(Page 6)