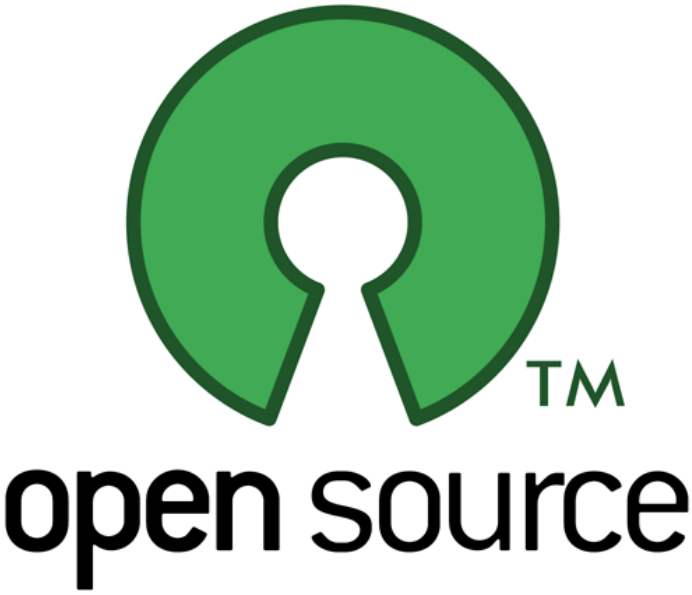
Açık Kaynak Kodlu Güvenlik Yazılımları – Ag Tarama Araçları



Açık kod dünyasında uzun zamandır kullanılan, belli bir kararlılığa ulaşmış ve ilgili konuda kendini ispatlamış birçok güvenlik yazılımı vardır. Bu yazılımlar: korunma, saldırı ve test araçları, izleme, şifreleme araçları vs gibi çeşitli kategorilere ayrılırlar.

Her bir kategoride birbirine benzeyen onlarca araç ve her aracı tercih eden farklı müdavimleri vardır. Yaptığım kısa bir araştırma sonucu belirli kullanıcı kitlesine sahip yaklaşık 800 adet açık kodlu güvenlik yazılımının var olduğunu tespit ettim. İşin güzel tarafı bu kadar zengin seçenek sunan bu yazılımlar için bizden talep edilen hiçbirşey yok!

Burada hatırlatılması gereken önemli bir nokta var ki o da açık kaynak kodlu araçların birer "ürün" degil proje olduğudur. Bu sebeple genelde piyasada bulunan muadili ürünlere oranla teknik olarak eksiklikleri olmasa da kullanım kolaylığı, esneklik ve birinci elden ticari destekleri eksiktir. Bu da tüm sorumluluğun yazılımı kullanana ait olması demektir.

Bu ve bundan sonraki sayılarda çeşitli kategorilerde güvenlik araçlarını bu köşeye alarak inceleyeceğiz. Kimi zaman incelemeler teorik ve yüzeysel, kimi zaman da olabileceğine teknik ve pratiğe yönelmiş olacak. Sizlerden gelecek tavsiye ve eleştirileri de değerlendirerek uzun vadede açık kaynak kodlu güvenlik yazılımları kütüphanesi kuracağımıza inanıyorum.

Ağ tarama ve Paket üretim araçları

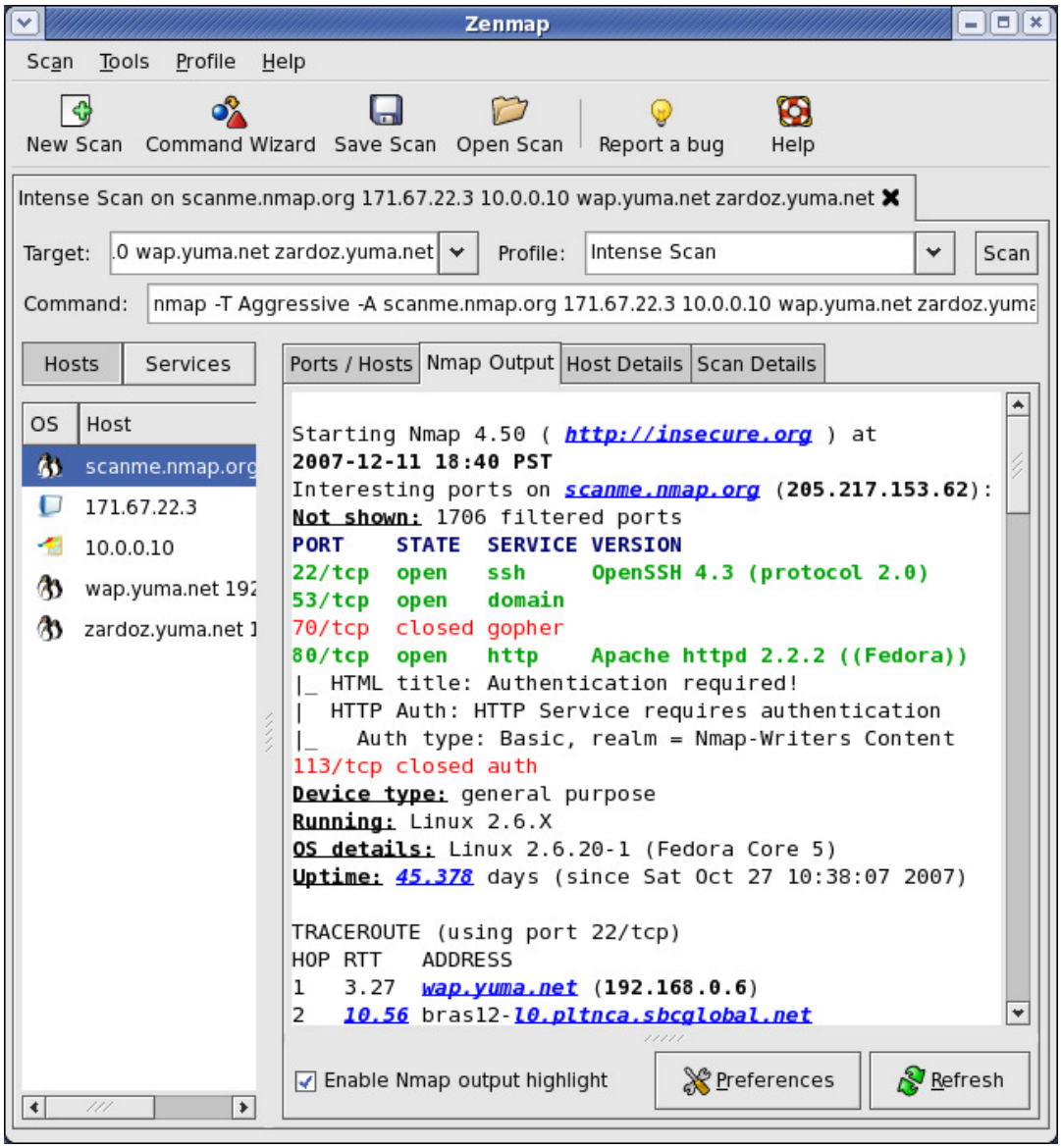
Nmap

"Bir cümlenin içerisinde "tarama" kelimesi geçiyorsa o cümlede mutlaka nmap'in de ismi geçer" özlü sözüne uyarak ben de ilk yazımda Nmap'e yer verdim.
Yazıyı hazırlarken bir arkadaşımın "yine mi Nmap?" serzenişini en son Nmap'in sitesini ne zaman kontrol ettin cevabı ile yatıştırdım ve Eylül ayında çıkan 4.76

sürümündeki özelliklerden bahsettim. Kısa bir sure sonra tatmin olmuş olmali ki hemen yeni sürümü grafik arabirimi ile indirerek kurcalamaya başladı.

Nmap(Network Mapper) çok amaçli ag arastirma ve port tarama aracidir. Kolay kullanimi ve sundugu esnek özellikler yillardir NMAP'i güvenlik dünyasinda hakli bir yere oturtmustur. Geliştiricisi Fyodor Arkin Nmap'e özel önem vererek mesaisinin önemli bir kısmını geliştirme için harcadığını söylüyor.

Nmap, sistemini komut satırından kullanmaya alışmış UNIX uzmanlarına hitap ettiği gibi komut satırına hiç bulasmadan kullanmak isteyen kullanıcılar için de oldukça basit ve anlaşılır bir grafik arabirim sunar. Ve en güzeli de Windows ortamında çalışabilir.



Nmap hakkında –başta kendi sitesi olmak üzere- çeşitli yazılar ve kitaplar yayınlanmıştır. Bu yazılara Google üzerinden yapılacak kısa bir araştırma ile erişilebilir. Fakat tavsiyem okumakla kalmayıp birebir okuduklarınızı –kendi sorumluluk alanınızda olan sistemler üzerinde- denemeniz.

Nmap ile yapılabilecek bazı işlemler;

- Çesitli Port tarama tekniklerini destekler
  UDP, TCP connect(), TCP SYN (half open), ftp proxy(bounce attack), ICMP (ping sweep), FIN, ACK sweep, Xmas Tree, SYN sweep, IP Protocol, Null scan,
- TCP/IP fingerprint ile isletim sistemi saptama
- Paralel port tarama
- Çalisan servis tipi ve versiyonu belirleme
- Uptime süresi belirleme

Portların durumu hakkında detay bilgi

Port taramaları yaparken portların durumu hakkında Nmap duruma gore Open, Filtered, Closed gibi terimler kullanır fakat çoğu kullanıcı bunların ne manaya geldiğini anlamaz. Bir portun durumu hakkında detay bilgi almak için Nmap'I –reason parametresi ile çalıştırmak yeterli olacaktır.

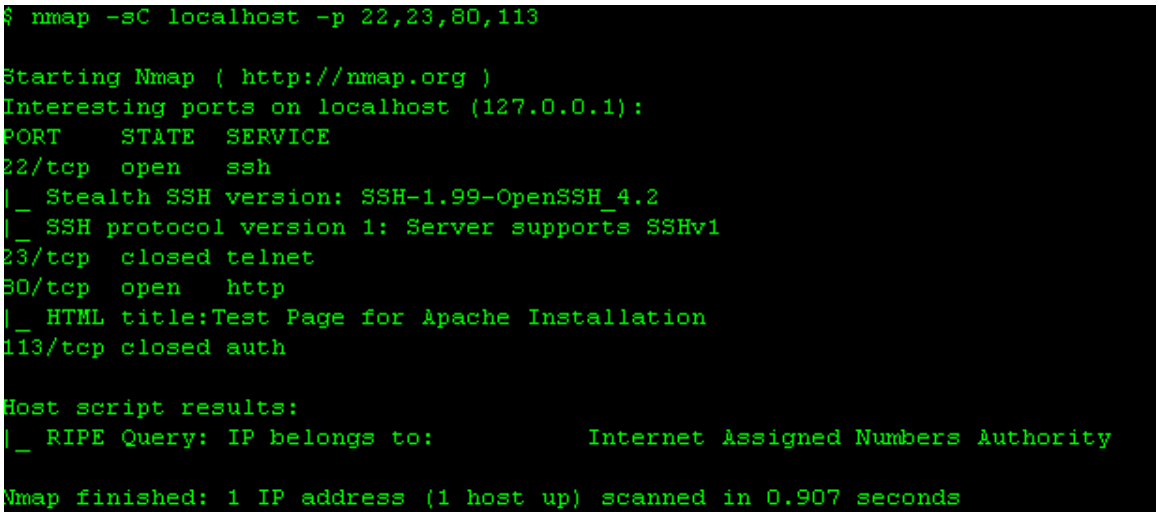
#nmap scanme.nmap.org –reason

```
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 994 filtered ports
Reason: 994 no-responses
PORT    STATE  SERVICE REASON
22/tcp  open   ssh     syn-ack
25/tcp  closed smtp    reset
53/tcp  open   domain  syn-ack
70/tcp  closed gopher  reset
80/tcp  open   http    syn-ack
113/tcp closed auth    reset

Nmap done: 1 IP address (1 host up) scanned in 4.21 seconds
```

Nmap Scripting Engine

Nmap'in yeni sürümleri ile birlikte gelen kullanışlı özelliklerden biri de NSE(Nmap Scripting Engine). NSE, lua dili kullanılarak Nmap'e taramalarda ek scriptler kullanabilme özelliği kazandırıyor. Bu özellikle birlikte Nmap'in ag/port tarama aracı kategorisinden taşıp zayıflık tarama kategorisine de adım attığı söylenebilir.



Nmap'in port tarama konusundaki en temel eksikliklerinden biri UDP taramaları sonuclarında oldukca yanıltıcı olmasıdır. Bunun sebebi UDP protokolünde yatmaktadır.

Normal tarama programları(Nmap dahil) udp portlarını tararken portun durumunu gelen/gelmeyen cevaba göre açıklar. Normal tarama programları udp taraması yaparken hedef udp portuna boş udp paketleri gönderir. Eger cevap gelmezse portun açık olduğunu -ya da filtrelenmis oldugunu- kabul eder. Cevap olarak icmp paketi alırsa portun kapalı -ya da filtrelenmiş olduğunu- varsayar. Bu gibi durumlarda Nmap'in –sV parametresi ya da Unicornscan gibi bu iş için düşünülmüş alternatif tarama programlarının kullanımı daha dogru sonuçlar verecektir.

Hping

Hping, istenilen türde TCP/IP paketleri olusturmak için kullanilan harikulade bir araçtir. Ismi ping programından esinlenilmesine rağmen ping programı gibi sadece icmp echo paketleri ile degil icmp, tcp, udp raw-ip protokolleri üretmek için kullanılabilir.

Olusturulacak paketlerde tüm alanların kendimize özgü belirlenebilmesi, dinleme modu ile hostlar arasi dosya transferi ve komut çalistirma özelligi(Truva ati?), IDS/IPS testleri için özel veri alanı belirtilebilmesi(ids imzalarinin testi) gibi ileri düzey özelliklere sahiptir.

Hping'i tüm özellikleri ile efektif kullanabilmek , çiktilarini yorumlamak için orta düzey TCP/IP bilgisi gerekir. Klasik otomatize araçlardan farkli olarak hping ile tamamen kendi olusturdugunuz (tcp/ip bilgisi burada ise yariyor) paketleri aga gönderirsiniz. Mesela XMAS Scan için nmap'de nmap –SX komutu verilirken hping'de XMAS scanin ne oldugunu, hangi TCP bayraklari ile gerçeklestirildigini bilmeniz ve ona göre parametreleri olusturmaniz gerekir (hping –FUP hedef_sistem gibi)

Hping'in kullanim amaçlarindan bazilari asagidaki gibidir,

- Ates duvari kural testleri
- Gelismis port tarama
- Gelismis traceroute
- Isletim sistemi saptama
- DDOS testleri
- Uzak sistemlerin uptime surelerini belirleme
- TCP/IP yigin testi,

Hping Kullanım Örnekleri:

Hping'e herhangi bir parametre vermezseniz icmp yerine TCP paketlerini kullanır. Boş(herhangi bir bayrak set edilmemiş) bir tcp paketini hedef sistemin 0 portuna gönderir ve gelen cevabı ekrana basar. TCP paketleri yerine udp, icmp ya da ip paketleri göndermek isterseniz –udp, --icmp, --raw-ip seçeneklerini denemelisiniz.

TCP bayraklarını belirtmek için her bayrağın ilk harfini yazmak yeterli olacaktır. Mesela 192.168.1.1 ip adresinin 80. portuna RST bayraklı tcp paketleri göndermek için aşağıdaki gibi bir komut yeterli olacaktır.

#hping -R -c 3 192.168.1.1 –p 80

HPING 192.168.1.1 (eth0 192.168.1.1): R set, 40 headers + 0 data bytes ---
192.168.1.1
hping statistic --- 3 packets tramitted, 0 packets received,
100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms

Hping ile port tarama

Hping ile yapılacak ve düzenli sonuç üretecek port tarama için –scan parametresi kullanılır.

#hping --scan 21,22,23,80,110,130-143 -S 14.7.2.88
Ilgili hostun 21,22….ve 130 ile 140.portları arasına SYN tarama yapılır.

XMAS Scan

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 tek satirda XMAS taraması yapabiliriz.

#hping –FUP hedef_sistem -p 80

Firewall Performans Testleri (DDOS Saldırısı Oluşturmak)

DDOS saldırılarında amaç olabildiğince fazla sayıda ve olabildiğince farklı kaynaktan hedef sisteme paketler göndererek hattın/sistemin kapasitesini doldurmasını ve yeni bağlantı kabul etmemesini sağlamaktır.

Bunun için genellikle büyük boyutlu udp paketleri kullanılır fakat SYN bayrağı set edilmiş ve kaynak ip adresi random olarak atanmış binlerce paket göndererek de (Syn

Flood)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

HPING 192.168.1.3 (eth0 192.168.1.3): S set, 40 headers + 0 data bytes hping in flood mode, no replies will be shown ...
```

IDS/IPS Testlerinde Hping

Hping'in bir özelliği de oluşturulacak paketlere istenen verinin payload olarak eklenebilmesidir. Bu özelliği kullanarak ağımızda kullandığımız IDS/IPS sistemlerini test edebiliriz.

Mesela içeriği

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

Şeklinde olan bir dosyayı –E parametresi ile kullanarak hedef sistemin 80. portuna gönderdiğimizde aradaki IDS/IPS sisteminin uyarı vermesi gerekir. Bu ve bunun gibi çeşitli örnekleri bularak ids sistemleri basitce teste tabi tutulabilir.