NMAP TRÊN KALI LINUX

Nmap là gì ?

- Nmap (Network Mapper) là một công cụ quét, theo dõi và đánh giá bảo mật một hệ thống mạng được phát triển bởi Gordon Lyon (hay còn được biết đến với tên gọi Fyodor Vaskovich).
- Nmap được công bố lần đầu tiên vào tháng 9 năm 1997.
- Nmap là phần mềm mã nguồn mở miễn phí, ban đầu chỉ được phát triển trên nền tảng Linux sau đó được phát triển trên nhiều nền tảng khác nhau như Windows, Solari, Mac OS… và phát triển thêm phiên bản giao diện người dùng (zenmap).

Các chức năng của Nmap:

- Phát hiện host trong mạng.
- Liệt kê các port đang mở trên một host.
- Xác định các dịch vụ chạy trên các port đang mở cùng với phần mềm và phiên bản đang dùng.
- Xác đinh hệ điều hành của thiết bị.
- Chạy các script đặc biệt.

Cài đặt Nmap

- Mặc định trong Kali Linux đã có sẵn công cụ Nmap
- Đối với người dùng, ta có thể truy cập http://nmap.org để tải về cài đặt phần mềm Nmap

Hướng dẫn Scan port với NMap

+ Xác định mục tiêu

Việc đầu tiên khi sử dụng nmap là xác định mục tiêu cần quét, mục tiêu có thể là 1 domain, 1 địa chỉ IP cố định, 1 dải địa chỉ IP, Ví dụ:

Quét 1 IP	nmap 192.168.1.1
Quét 1 dải IP	nmap 192.168.1.1/24
Quét 1 domain	nmap google.com

+ Các lệnh phổ biến trong Nmap

1, Quét hệ điều hành của Server

```
nmap -O remote_host
```

2, Quét một mạng rộng hơn

```
nmap -sP network_address_range
```

3, Quét mà không tra cứu DNS (Điều này sẽ giúp bạn quét nhanh hơn)

```
nmap -n remote_host
```

4, Quét một port cụ thể thay vì quét chung các port thông dụng

```
nmap -p port_number remote_host
```

5, Quét kết nối TCP, Nmap sẽ thực hiện việc quét bắt tay 3 bước

```
nmap -sT remote_host
```

6, Quét kết nối UDP

```
nmap -sU remote_host
```

7, Quét TCP và UDP từng port (Khá lâu để hoàn tất)

```
nmap -n -PN -sT -sU -p- remote_host
```

8, Quét TCP SYN scan (-sS):

```
nmap -sS remote_host
```

9, Quét vời các cờ -sN, -sF, -sX

```
nmap -PN -p port_number -sN remote_host
```

10, Quét xác định phiên bản của dịch vụ đang chạy trên host

```
nmap -PN -p port_number -sV remote_host
```

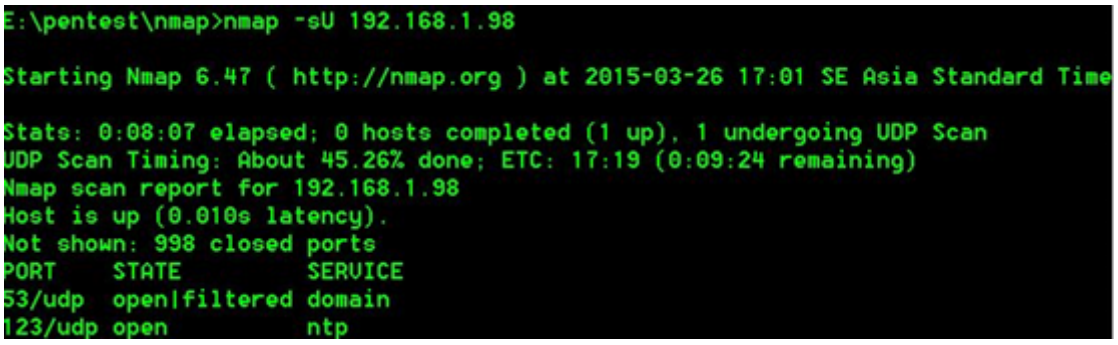
Chi tiết về các kĩ thuật quét

TCP SYN scan (-sS): Nmap gửi một gói tin TCP-SYN tới 1 port của mục tiêu. Nếu nhận được ACK_SYN thì port đó đang ở trạng thái open, nmap sẽ gửi gói tin RST để đóng kết nối thay vì gửi ACK để hoàn tất quá trình bắt tay 3 bước (vì thế kỹ thuật này còn được gọi là half open scan). Nếu nhận được RST thì port đó ở trạng thái close. Nếu sau 1 số lần gửi mà không nhận được trả lời hoặc nhận được ICMP type 3 (unreachable error) thì port đó ở trạng thái filtered

(đã bị firewall chặn).

TCP connect scan (-sT): Kỹ thuật này cho kết quả tương tự như TCP SYN scan, nếu nhận được ACK-SYN nmap sẽ gửi gói tin ACK để hoàn tất quá trình bắt tay 3 bước. TCP connect scan được dùng khi user không có quyền truy cập raw packet để thực hiện SYN scan (thường thì với quyền root trên linux mới có thể sử dụng SYN scan). TCP connect scan sẽ sử dụng TCP stack của hệ điều hành để tạo ra 1 kết nối bình thường với mục tiêu, do thực hiện 1 kết nối đầy đủ nên kỹ thuật này dễ bị phát hiện bởi hệ thống log của mục tiêu do đó SYN scan thường được sử dụng nhiều hơn để tránh bị phát hiện.

UDP scan (-sU): Nmap gửi gói tin UDP tới 1 port của mục tiêu nếu nhận được gói tin ICMP port unreachable error (type 3, code 3) thì port đó ở trạng thái close. Nếu nhận được ICMP unreachable errors (type 3, codes 1, 2, 9, 10, or 13) thì port đó ở trạng thái filtered. Nếu không nhận được gì thì port ở trạng thái open|filtered. Nếu nhận được gói tin UDP thì port đó ở trạng thái open



TCP NULL, FIN, and Xmas scans (-sN, -sF, -sX): Đây là kỹ thuật sử dụng các gói tin TCP với không có cờ nào được bật cờ FIN được bật cờ FIN, PSH và URG được bật 3 kỹ thuật này được gộp chung vào 1 nhóm vì chúng cho kết quả giống nhau. Khi 3 loại gói tin này được gửi đi nếu nhận được RST thì port ở trạng thái close, nếu nhận được các loại gói tin ICMP (type 3, code 1, 2, 3, 9, 10, or 13) thì port ở trạng thái filtered, còn nếu không nhận được gói tin trả lời thì port ở trạng thái open|filtered

```
E:\pentest\nmap>nmap -sF 192.168.1.98

Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-26 16:14 SE Asia Standard Time

Nmap scan report for 192.168.1.98
Host is up (0.0036s latency).
Not shown: 995 closed ports
PORT     STATE         SERVICE
23/tcp   open|filtered telnet
80/tcp   open|filtered http
444/tcp  open|filtered snpp
8000/tcp open|filtered http-alt
8008/tcp open|filtered http
```

Ngoài ra nmap còn có 1 số tùy chọn với các kỹ thuật khác nâng cao (-sY,-sM, -sO, -sZ, -sI) có thể tham khảo thêm tại http://nmap.org/book/man-port-scanning-techniques.html

+ **Lựa chọn port và thứ tự quét.** Mặc định nmap sẽ quét 1000 port phổ biến nhất (xem tại file nmap-service) với thứ tụ ngẫu nhiên.

Tùy chọn –p : lựa chọn chính xác các port cần quét, nếu quét đồng thời nhiều giao thức thì thêm các chữ cái đứng trước số port

T: TCP, U: UDP, S: SCTP, or P: IP Protocol.

Ví dụ:

```
E:\pentest\nmap>nmap -sS -sU -p U:53,4000,T:1-100,8000-8010,444 192.168.1.98

Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-26 16:59 SE Asia Standard Time

Nmap scan report for 192.168.1.98
Host is up (0.0028s latency).
Not shown: 108 closed ports
PORT     STATE    SERVICE
23/tcp   filtered telnet
80/tcp   open     http
444/tcp  filtered snpp
8000/tcp open     http-alt
8008/tcp open     http
53/udp   open     domain
```

Trong trường hợp này nmap sẽ quét các port UDP 53 và 4000, quét các port TCP 444, từ 1 đến 100, từ 8000 đến 8010 bằng kỹ thuật SYN scan.

Tùy chon –F (Fast scan): nmap quét 100 port phổ biến nhất thay vì mặc định 1000 port.

Tùy chọn –top-ports : quét n port phổ biến nhất.

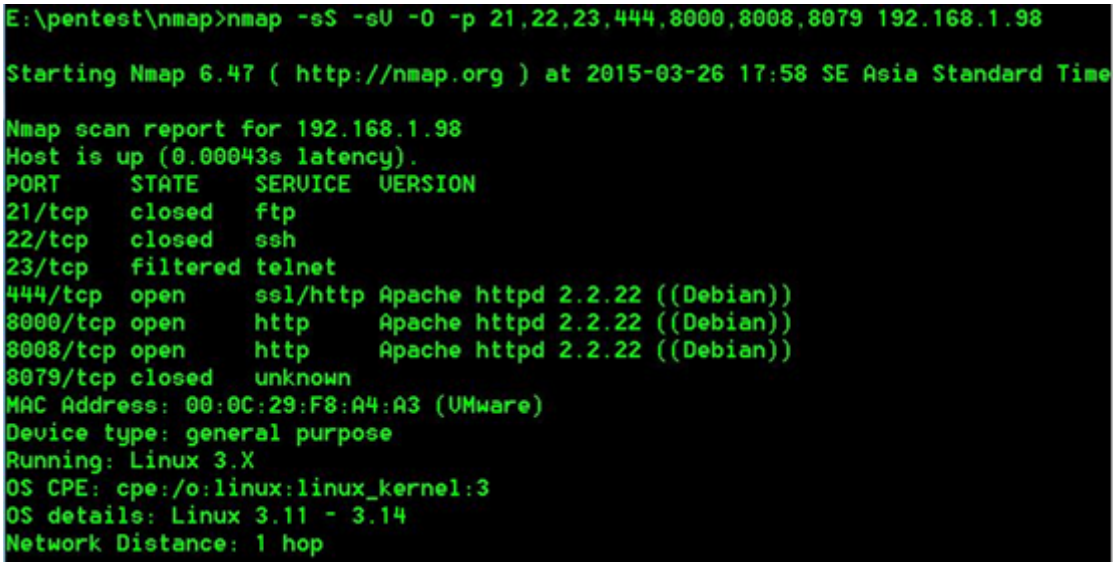
Tùy chọn –r: thứ tự quét các port từ thấp lên cao thay vì mặc định là ngẫu nhiên.

+ Xác đinh dịch vụ, phiên bản, hệ điều hành. Mặc định sau khi quét các port, nmap sẽ xác định dịch vụ đang chạy trên các port dựa vào file nmap-services (các port mặc định của từng service) tuy nhiên một số server cấu hình các dịch vụ không chạy trên các cổng mặc định. Để xác định rõ port nào chạy dịch vụ nào nmap sử dụng tùy chọn –sV. Với tùy chọn này nmap sẽ xác định được dịch vụ và phiên bản phần mềm chạy trên từng port dựa vào banner khi kết nối với port đó

Các port và dịch vụ tương ứng nmap xác định dựa trên port mặc định.

Các port và dịch vụ, phiên bản phần mềm nmap xác định khi có tùy chọn –sV

Ở trên nmap xác định port 444 chạy https thay vì mặc định snpp. Nmap hỗ trợ việc xác định hệ điều hành bằng tùy chọn –O. Nmap xác định hệ điều hành dựa trên TCP/IP stack fingerprint của mục tiêu (ví dụ như Sequence Number, window size, các Options và thứ tự của chúng trong TCP header, Identification number trong IP header, …). Có thể tham khảo thêm tại http://nmap.org/book/man-os-detection.html



+ Nmap hỗ trợ chạy các script đặc biệt:

Nmap Scripting Engine (NSE) là một trong những chức năng linh hoạt và mạnh mẽ nhất của Nmap. Nó cho phép người dùng viết và chia sẻ những đoạn script đơn giản để thực hiện những công việc khác nhau trong lĩnh vực networking một cách tự động. Những đoạn script có thể sử dụng để phát hiện các lỗ hổng, thậm chí khai thác các lỗ hổng. Các script (.nse file) nằm trong thư mục script khi cài đặt nmap, người dùng có thể tùy biến chỉnh sửa, thêm các scirpt khác. Để thực hiện chức năng này của nmap sử dụng tùy chọn

```
-script |||[,...]
```

Đánh giá về Nmap:

Linh hoạt: Hỗ trợ hàng chục kĩ thuật tiên tiến, dễ dàng vượt qua các bộ lọc từ hệ thống như các bộ lọc IP, tường lửa, bộ định tuyến và một số bộ lọc khác. Bao gồm cả cơ chế quét port (TCP và UDP), phát hiện hệ điều hành, phát hiện phiên bản, quét ping và nhiều hơn thế nữa.

Mạnh mẽ: Nmap được sử dụng để quét hệ thống mạng lớn với hàng trăm ngàn máy tính.
Di động: Hầu hết các hệ điều hành đều được hỗ trợ bao gồm cả Linux, Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga…
Dễ sử dụng: Nmap cung cấp nhiều tính năng từ đơn giản nhất như cú pháp "nmap -v -A targethost" đến những tính năng tiên tiến nhất cho người dùng. Qua cả command-line truyền thống và giao diện đồ họa (GUI) có sẵn vào tùy chọn theo sở thích của người dùng. Binary có sẵn cho những ai không muốn biên dịch Nmap từ mã nguồn.

Miễn phí: Mục tiêu chính của dự án Nmap là giúp cho mạng Internet ngày càng bảo mật hơn cũng như cung cấp cho các quản trị viên/kiểm thử viên/hacker có môt công cụ tiên tiến khám phá mạng của họ. Nmap tải về miễn phí, và kèm theo đó là mã nguồn bạn có thể chính sửa và phân phối lại theo các điều khoản được phép.