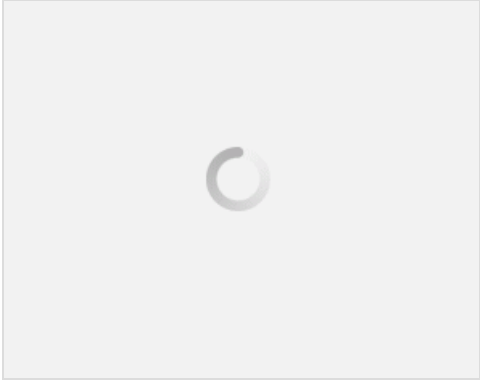
آموزش و معرفی انواع پورت اسکن (Port Scan) در کالی لینوکس قسمت ۱ (نسخه PDF)

سلام به دوستان عزیز ITPro ای و علاقه منـدان به مباحث امنیت شـبکه. در قسـمت قبل توانستیم قسـمت اول از بحث اسـکن پورت در لینوکس کالی را خدمت شـما دوستان عزیز بیان کنیم و در این بخش میخواهیم تا با ارائه جزئیات بیشتری از این موضوع، تبحر شما را در کار کردن با لینوکس کالی بیشتر کنیم. با ما همراه باشید:

مشکلات رایج در Port Scanning



- UDP Port Scanning معمولا قابل اطمینان نیست. چرا که فایروال ها و روترها ممکن است در بین راه پکت های ICMP را دراپ کنند (از بین ببرند). این موضوع میتوانند باعث ایجاد نتایج مثبت اشـتباه در خروجی شود و شما بطور مرتب در اسکن پورت های UDP مشاهده کنید که تمام این پورت ها در سیستم تحت اسکن، باز هستند.
- اکثر اسـکنرهای پورت تمام پورت های ممکن را اسـکن نمیکننـد. این نرم افزارها معمولا لیستی از پیش تعیین شـده از پورت های پرکاربرد دارند که فقط بر اساس آن ها اسکن را انجام میدهند.
- کـاربران معمولا فراموش میکننـد که پورت های UDP را اسـکن کرده و معمولا فرآینـد اسـکن را محدود به پورت های TCP میکنند. بنابراین در نتیجه به خروجی آمده، فقط نیمی از پورت های ممکن را خواهند دید.

Port Scanning با Nmap

Nmap یکی از نرم افزارهای اسـکنر محبوب، همه کاره و قدرتمند در دنیای امروز است. این نرم افزار بیش از یک دهه است که از توسعه آن میگذرد و خصوصیات متعددی را در پشت ظاهر ساده خود دارد. در ادامه قصد داریم تا در این رابطه چند مثال را بیان کنیم تا پس آن در کار کردن با این نرم افزار احساس راحتی کنید!

پاسخگو در برابر ترافیک شما

اسکن پورت های TCP در Nmap، حدود ۱۰۰۰ پورت معروف را در سیسـتم مورد نظر شناسایی و اسکن میکند. قبل از آن که اقدام به اجرای اسـکن کنیم، میخواهیم مقدار ترافیک ارسالی ناشـی از یک اسکن ساده را مشاهده کنیم. برای این کار یکی از سیستم های لوکال را اسکن کرده و میزان ترافیک ارسالی به سیسـتم مورد نظر را با اسـتفاده از "iptables" مانیتور خواهیم کرد.نکته:iptables یک برنامه در فضای خط فرمان (command line) است که در ساختاربنـدی و کانفیگ مجموعه قوانین فیلترینگ پکت در لینوکس x.۲.۴ و بعد از آن استفاده میشود. این برنامه جهت استفاده مدیران طرح ریزی شده است.

```
root@kali:~# iptables  -I INPUT 1 –s 10.0.0.19 –j ACCEPT
root@kali:~# iptables –I OUTPUT 1 –d 10.0.0.19 –j ACCEPT
root@kali:~# iptables –Z
root@kali:~# nmap –sT  10.0.0.19


Starting Nmap 6.25 (http://nmap.org) at  2015-05-20 06:36  EDT
```

```
Nmap scan report for 10.0.0.19
Host is up (0.00048 s latency).
Not shown: 986 closed ports
PORT  STATE SERVICE
21/tcp  open ftp
23/tcp  open telnet
25/tcp  open smtp
135/tcp  open msrpc
1*39/tcp  open netbios-ssn
445/tcp  open Microsoft-ds
515/tcp  open printer
3389/tcp open ms-wbt-server
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49157/tcp open unknown
MAC Address: 00:C:29:3B:C8:DE (VMware)


Nmap done: 1 IP address (1 host up) scanned in 1.91 seconds


root@kali:~# iptables  -vn –L
chain INPUT (policy ACCEPT 10 packets, 464 bytes)
pkts bytes  target  prot opt   in  out  source  destination
1002 40400 ACCEPT  all     --     * *  10.0.0.19 0.0.0.0/0
0 0 ACCEPT  all     --      * *  10.0.0.19 0.0.0.0/0

Chain OUTPUT  (policy ACCEPT 4 packets, 1052 bytes)
Pkts  bytes  target   prot   opt   in  out  source  destination
1201 71796 ACCEPT  all       --     * *  0.0.0.0/0 10.0.0.19

root@kali:~#
```

این اسکن ۱۰۰۰ پورت فقـط در قالب ۷۲ کیلوبـایت ترافیـک انجام شـده است. این در حالی است که یک پورت اسـکن ساده تمام ۶۵۵۳۵ پورت موجود را جسـتحو و اسـکن کرده و چیزی در حدود ۴.۵ مگابایت ترافیک تولیـد میکنـد. علاوه بر این با انجام این اسـکن کامل دو پورت جدید از TCP را در نتایج مشاهده خواهیم کرد که در اسکن پیش فرض پورت های TCP به آن اشاره اغی نشده بود:

```
root@kali:~# iptables –Z
root@kali:~# nmap –sT –p 1-65535 10.0.0.19
Starting Nmap 6.25 (http://nmap.org)  at  2015-05-20   06:19  EDT
Nmap scan report for 10.0.0.19
```

```
Nmap scan report for 10.0.0.19
Host is up (0.00067 s latency).
Not shown: 65519 closed ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
25/tcp open smtp
135/tcp open msrpc
139/tcp open netbios-ssn
180/tcp open ris
445/tcp open Microsoft-ds
515/tcp open printer
3389/tcp open ms-wbt-server
25017/tcp open unknown
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
49157/tcp open unknown
MAC Address: 00:0C:29:3B:C8:DE (VMware)

Nmap done: 1 IP address (1 Host up) scanned in 80.42 seconds
root@kali:~# iptables -vn –L
chain INPUT (policy ACCEPT 54 packets, 2412 bytes)
pkts bytes target prot opt in out source destination
65540 2622K ACCEPT all -- * * 10.0.0.19 0.0.0.0/0
0 0 ACCEPT all -- * * 10.0.0.19 0.0.0.0/0

Chain OUTPUT (policy ACCEPT 12 packets, 3120 bytes)
pkts bytes target prot opt in out source destination
76206 4572K ACCEPT all -- * * 0.0.0.0/0 10.0.0.19
root@kali:~#
```

نتایج بالا این مفهوم را میرسانند که یک اسـکن کامل Nmap از یک شبکه کلاس C با ۲۵۴ هاست، میتواند در نتیجه ارسال ۱۰۰۰ مگابایت ترافیک در شبکه است. در بهترین وضعیت، یک اسکن کامل از پورت های TCP و UDP از یک سیستم تنها میتواند اطلاعات تقریبا دقیقی از سرویس هـای شـبکه ای در معرض خطر بما بدهـد. مثال بالا این ایـده را نیز بما میدهـد که اگر میخواهیم پورت ها و سـرویس های باز بیشتری را با اسـتفاده از یک اسـکن کامل تر، جسـتجو کنیم، نیاز داریم تا با متعادل سازی عوامل محـدود کننده انتقال ترافیک (مانند یک Uplink کند)، شـرایط را برای نیل به این هدف هموار سازیم. این موضوع مخصوصا برای شبکه های بزرگتر مانند شبکه های کلاس B بیشتر خود را نشان خواهد داد. اما اگر در موقعیتی هستیم که امکان اجرای یک پورت اسـکن کامل را بر روی شبکه نداریم، چکار میتوانیم انجام دهیم؟ در قسمت سوم از سری مباحث اسکن شبکه با کالی در این مورد و تکنیک های مرتبط صحبت خواهیم نمود. با ما همراه باشید.

سربلند و مانا باشید.

نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

مطلب اصلی