آموزش و معرفی انواع پورت اسکن (Port Scan) در کالی لینوکس قسمت ۲ (نسخه PDF)

سلام به دوستان عزیز ITPro ای. در ادامه سـری آموزش های تست نفوذ با لینوکس کالی، به مرحله اسکن پورت ها و شناسایی باز یا بسته بودن آن ها رسـیدیم. اگر بخواهیم بصورت خیلی عامیانه و کلی تعریفی داشته باشیم، باید بگوییم که **Port Scanning** فرآیند بررسی پورت های باز TCP یا UDP بر روی یک سیستم ریموت است. بخاطر داشته باشید که Port scanning در بسیاری از کشورها یک فرآیند غیر قانونی است و نباید در خارج از محیط آزمایشگاهی انجام شود. از جمله اخیر میتوان نتیجه گرفت که الان زمان انتقال فعالیت هایمان از فاز پسیو به اکتیو است که شامل فعالیت های مستقیم بیشتری بر روی سرورهای هدف میشود. قبل از شروع کار بسیار مهم است که چگونگی انجام port Scanning را درک کرده باشیم.

Connect Scanning چیست؟

ساده ترین تکنیک اسکن کردن پورت های TCP، به connect scanning معروف است که برپایه مکانیسم three-way handshaking کار میکند. بر طبق این مکانیسم، دو طرف ارتباط میتواننـد قبل از انتقال دیتا، با یکدیگر مذاکره کنند. در Connect port scanning بر روی پورت خاصی از سیسـتم هدف، تلاش برای اجرای فرآیند کامل three-way handshaking صورت میپـذیرد. اگر فرآیند مذکور بطور کامل اجرا شود، میتوان نتیجه گرفت که پورت مورد نظر باز میباشد.

```
root@kali:~# nc –nvv –w 1 –z 10.0.0.19 3388-3390
(unknown) [10.0.0.19] 3390 (?) : connection refused
(unknown) [10.0.0.19] 3389 (?) open
(unknown) [10.0.0.19] 3388 (?) : connection refused
Sent 0, rcvd 0
```

مثال زیر نمونه ای کپچر شده از یک TCP Netcat port scan را بر روی پورت های ۳۳۸۸ تا ۳۳۹۰ نشان میدهد:

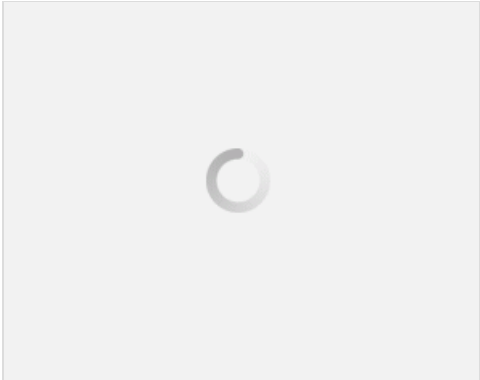
Stealth// SYN Scanning چیست؟

فرآیند SYN Scanning یک روش اسکن پورت های TCP است که شامل ارسال پکت های SYN به پورت های مختلف سیستم هدف بدون الزام به تکمیل مکانیسم ۳-way handshaking است. اگر یک پورت TCP باز باشد، سیستم هدف باید یک SYN-ACK را به مبداء ارسال کند که به ما این اطلاع را میدهد که پورت باز است؛ بنابراین دیگر نیازی به ارسال ACK نهایی به سمت سیستم هدف نمیباشد.

UDP Scanning چیست؟

از آنجایی که نوع وضعیت ترافیک در UDP مشخص نیست و شامل فرآیند three-way handshaking نمیشود، مکانیسم پس زمینه در UDP Port Scanning میتواند متفاوت باشد. سـعی کنید با اسـتفاده از وایرشارک و توسط netcat فرایند UDP Scanning را بر روی یک سیسـتم (سیستم تست) اجرا کنید تا نحوه کارکرد UDP Port Scan را بهتر متوجه شوید. تصویر زیر کپچری از وایرشارک را نشان میدهد که در آن با استفاده از netcat بر روی پورت های ۱۶۰ تا ۱۶۲ عمل UDP Port Scan را انجام داده‌ایم:

```
root@kali:~# nc –nv –u –z –w 1 10.0.0.19 160-162
(unknown) [10.0.0.19] 161 (snmp) open
```



از تصویر بالا میتوان متوجه شد که اسکن های UDP کاملا نسبت به اسکن های TCP متفاوت عمل میکنند. یک پکت خالی UDP به پورت خاصی میشود. اگر پورت UDP باز باشد، هیچ جوابیه ای از طرف سیستم هدف به مبداء ارسال نخواهد شد. در مقابل اگر پورت UDP بسته باشد، یک پکت ICMP با مضمون "port unreachable" از طرف ششستم مقصد به سیستم مبداء ارسال خواهد شد.

سربلند و مانا باشید.

نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

مطلب اصلی