آموزش Shodan : شناسایی اهداف هک و نفوذ در کالی لینوکس بخش ۴ (نسخه PDF)

در قسـمت پیش توانستیم بصورت خلاـصه با ابزار آنلاین Shodan و چرایی اسـتفاده از آن صـحبت کنیم. امـا همانطور که قولش را داده بودیم، در این بخش به معرفی وکار با قابلیت های Shodan می پردازیم. پس با ما همراه باشید:

وب‌سایت Shodan

برای استفاده از Shodan، در مرورگر آدرس اینترنتی "Shodanhq.com" را وارد کنید:

در مرحله بعـد تمام آن چیزی که شـما احتیاج داریـد اینست که کلمه یا عبارت کلیدی خود را در کار مخصوص جسـتجو وارد کرده و دکمه جستجو را بفشارید؛ عملیات جستجو طوری انجام خواهد شد که انگار شما این جستجو را با هر موتور جستجویی انجام داده اید! مثلا اگر ما بخواهیم روترهای سیسکو را جستجو کنیم، فقط باید در کادر مخصوص عبارت "Cisco" را تایپ کنیم و جستجو را شروع کنیم:

Shodan لینک های حدود ۲ میلیون روتر سیسـکو را در سراسـر جهان در اختیار شما خواهد گذاشت. شما میتوانید بر روی هرکدام از آدرس های IP کلیک کرده و بطور مستقیم در دیوایس پیدا شده، گشت و گذار نمایید. در قسمت چپ صفحه، Shodan بشما تعدادی از دیوایس های پیدا شده را نشان میدهد که توانسـته است محل و یا کشور دقیق آن را تشـخیص دهد. در این مرحله شـما میتوانید به نتایج نشان داده شده بسنده کنید و یا با استفاده از فیلترهای تعریف شده، نتایج جستجو را دقیقتر نمایید.

راهنمای فیلتر کردن

با استفاده از دستورات فیلتر شما میتوانید بسرعت نتایج جستجو را به آن چیزی که مد نظرتان است، محدود کنید. برای مثال شما کارمند مایکروسافت هستیـد و میخواهید تمام سـرورهای IIS را که از نسـخه ۸.۰ IIS اسـتفاده میکننـد و در آمریکـا و تحت دومین مایکروسافت هستند را پیدا کنید. برای جستجو شما باید عبارتی نظیر شکل زیر را وارد کنید:

جسـتجو این فیلتر بسـرعت و راحتی از میان میلیون های سـرور موجود، آن هایی را بشـما نشان خواهد داد که مطابق با درخواست شما باشند. در زیر نمونه ای از نتیجه برگردانده شده را خواهیم دید:

۱. ارائه اطلاعات از عنوان سرور. شما میتوانید دیگر سرورها را که دارای همین عنوان هستند را با قرار دادن اطلاعات در فرمان Title جستجو کنید.
۲. تعیین محل جغرافیایی (کشور) سرور. مجددا یاآور میشود که جستجو میتواند بر اساس فرمان Country نیز انجام شود.
۳. مفهوم جستجوی Hostname در جستجوی سرورهایی با نام دومین مشخص شده استفاده میشود.
۴. محدوده بدنه متن. هر متنی که در Shodan بدون فیلتر قرار گیرد، به این منزله تلقی میشود که باید آن را در میان بدنه متن جستجو کرد و در نتایج شاهد سرورهایی خواهیم بود که اطلاعات داده شده در بدنه متن آن قرار گرفته است.

دستورات فیلتری

در این بخش میخواهیم نگاه دقیقتری به دستورات فیلتری بیاندازیم.برای استفاده از این دستورات یا گرفتن بیش از یک صفحه نتیجه، باید بطور رایگان در سایت ثبت نام کرده و کار را با اکانت ثبت شده خود ادامه دهید.

دستور شهر و کشور

این دستور به شما اجازه میدهد تا نتیج جستجو را در محدود جغرافیایی خاصی محدود کنید.

Country: (کد اختصاری دو حرفی کشور) یا City: (نام شهر)

بطور مثال:

```
country:US
```

```
city:Memphis
```

اگر شهری که شما دنبالش میگردید، در بیش از یک کشور وجود دارد، بهتر است نام شهر و نام کشور را بصورت ترکیبی و با هم بیاورید:

```
US city-Memphis
```

دستور HOSTNAME

با این دستور میتوان کل یک دومین خاص را اسکن نمود:

```
google
```

شما میتوانید از بخشی از یک نام کامل دومین هم استفاده کنید، مصل google یا تمام نام آن را بیاورید، مثل www.microsoft.com یا support.microsoft.com.

دستور NET

یک آدرس IP خاص و یا یک رنج خاص در شبکه را با استفاده از این دستور اسکن میکند:

```
Net:192.168.1.10
```

```
Net:192.168.1.0/24
```

دستور TITLE

شما میتوانید موارد دلخواه خود را با استفاده از دستور Title جستجو کنید:

```
"Title:"Server Room
```

Title یا عنوان احتمالا یکی از پارامترهای جستجو باشد که بیشتر در معرض دید قرار دارد. شما میتوانید تمام اینترنت و یا تمام یک

دومین را بر اساس یک کلمه کلیدی جستجو کنید.

جستجوی کلمه کلیدی

احتمالا یکی پرطرفدارترین راه جستجو در Shodan استفاده از جستجوی کلمه کلیدی متن است. اگر شما نوع سرور مورد استفاده در سیستم مقصد را میدانید، نام سرور را جستجو کنید.برای مثال اگر بخواهید تمام سرورهایی که از وب سرور Apache نسخه ۲.۲.۸ استفاده میکنند و سایت های باز باشند یا در جواب پیغام خطا بر نگردانند (سایت های ۲۰۰ OK)، را جستجو کنید، باید از کلمات کلیدی زیر استفاده کنید:

```
Apache//2.2.8 200 ok
```

یا شاید بخواهید در نتایج بدست آمده هرگونه سایت دارای پیغام ۴۰۱ unauthorized pages یا ۳۰۲ Moved pages را حذف کنید. بنابراین باید از علامت "-" و کد خطای HTML استفاده کنید:

```
Apache//2.2.8 -401 -302
```

خوب دوستان در این بخش نیز توانستیم با دستورات فیلتری در Shodan آشنا شویم. اما کار به اینجا ختم نمیشود و ابزار آنلاین Shodan حرف های بیشتری برای گفتن دارد. بنابراین اگر این آموزش ها را دنبال میکنید، در بخش بعد نیز با ما همراه باشید.سربلند و مانا باشید.

پایان بخش دوم

نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

مطلب اصلی