بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

راهنمای استفاده از اسکنر log4jScanner

گزارش فنی

شناسه سند	log4jScanner_manual_14001007
نوع سند	گزارش فنی
شماره نگارش	۱
تاریخ نگارش	۱۴۰۰/۱۰/۱۵
طبقه‌بندی سند	محرمانه


تهران- میدان آرژانتین- ابتدای بلوار بیهقی- نبش خیابان شانزدهم- ساختمان شماره ۱ سازمان فناوری اطلاعات ایران


(۰۲۱)۴۲۶۵۰۰۰۰


۰۲۱ ۴۲۶۵۰۰۰۰


uucert.com

فهرست مطالب

۱ پیش‌نیازهای استفاده از اسکنر log4jScanner

ابزار پیش رو برای اسکن آسیب‌پذیری موجود در کتابخانه log4jScanner به صورت از راه دور به کار گرفته می‌شود که در ادامه پیش‌نیازهای استفاده از آن آمده است.

۱-۱ پیش‌نیازهای سیستمی

۱-۱-۱ سیستم عامل

این ابزار به صورت کامپایل شده برای سیستم عامل‌های ویندوز و لینوکس ۶۴ بیتی آماده شده است و بنابراین تنها بر روی این سیستم عامل‌ها قابل استفاده است.

- برای سیستم عامل ویندوز وابستگی خاصی مورد نیاز نبوده و فایل log4jScanner.exe قابل اجرا است.
- برای سیستم عامل لینوکس احتمالا هنگام اجرای برنامه پیغام خطای برخی وابستگی‌ها از جمله خطای نسخه GLIBC نشان داده شده و برنامه اجرا نشود که در این صورت بایستی نسخه متناسب با برنامه نصب شود.

۱-۱-۲ سطح دسترسی

برای استفاده از این ابزار بالاترین سطح دسترسی مورد نیاز است. بنابراین کاربر استفاده کننده از این اسکنر بایستی در محیط ویندوز دسترسی به سطح Administrator و در محیط لینوکس دسترسی به سطح root داشته باشد تا بتواند اسکنر را اجرا کند.

۱-۲ پیش‌نیازهای شبکه

۱-۲-۱ آی‌پی

برای شناساندن آی‌پی مناسب به برنامه، اطلاع داشتن از آی‌پی سیستم مورد نیاز است. برنامه به صورت پیش فرض یکی از آی‌پی‌ها سیستم را به عنوان آی‌پی اسکنر در نظر می‌گیرد اما اگر سیستم اسکنر دارای چندین کارت شبکه و آی‌پی مختلف باشد احتمال خطا وجود دارد بنابراین مشخص کردن آی‌پی سیستم به صورت شفاف توصیه می‌شود. اگر اسکنر برای اسکن آی‌پی‌های داخل شبکه استفاده می‌شود باید آی‌پی داخل شبکه مورد استفاده قرار بگیرد. اما اگر از این ابزار برای اسکن آی‌پی‌های خارج از شبکه و بر روی بستر اینترنت استفاده می‌شود باید آی‌پی پابلیک را به عنوان آدرس سرور به ابزار داد.

۲-۲-۱ پورت

این ابزار برای اسکن آی‌پی‌های مورد هدف نیازمند گوش دادن به پورت TCP 1389 برای کانکشن‌های LDAP و پورت UDP 53 است. بنابراین اولا باید از اینکه سرویس یا برنامه دیگری از این پورتها استفاده نمی‌کند اطمینان حاصل کرد و ثانیا از تنظیمات فایروال اجازه برقراری ارتباط با این پورت‌ها از بیرون داده شود. همچنین اگر از این اسکنر برای اسکن آی‌پی‌های خارج از شبکه استفاده می‌شود باید مطمئن شد که فایروال روتر اجازه استفاده از این پورت‌ها را برای این سیستم می‌دهد. در صورت لزوم باید port forward صورت بگیرد.

۲ راهنمای اجرای اسکنر log4jScanner

این ابزار برای استفاده در محیط ترمینال تهیه شده است. بنابراین برای استفاده در محیط ویندوز باید از Command Prompt یا Windows PowerShell و در محیط لینوکس از یکی از شبیه‌سازهای ترمینال مانند Gnome Terminal استفاده شود.

- در محیط لینوکس دقت شود که ابزار بدون دسترسی روت اجرا نخواهد شد و بنابراین باید sudo قبل از اجرای برنامه به کار گرفته شود.
- در محیط ویندوز دقت شود که ترمینال به صورت Run As Administrator اجرا شود.

پس از اجرای ترمینال وارد پوشه حاوی فایل اجرایی خواهیم شد.

شکل کلی اجرای برنامه به صورت زیر است:

فرض کنیم آی‌پی سیستمی که در آن اسکنر اجرا می‌شود 192.168.1.100 است و می‌خواهیم تمامی آی‌پی‌های موجود در زیرشبکه خود را از 192.168.1.1 تا 192.168.1.254 اسکن کنیم. دستور اجرایی در محیط ویندوز به صورت زیر خواهد بود:

```
log4jScanner.exe scan --cidr=192.168.1.0/24 --ldap-server=192.168.1.100:1389
```

نکاتی در خصوص دستور:

- دستور scan برای اجرای اسکن مورد نیاز است.
- اگر تنها اسکن یک آی‌پی خاص مدنظر باشد می‌توان به جای cidr– از ip-- استفاده کرده و آی‌پی مورد نظر را تعیین کرد. همچنین اگر آی‌پی‌های هدف به صورت یک لیست در فایلی متنی قرار داشته باشند می‌توان با استفاده از list– این لیست را به برنامه تعریف کرد. آی‌پی‌ها در داخل این فایل باید به نحوی باشند که در هر خط یک آی‌پی قرار داشته باشد.

- همانگونه که اشاره شد، در این سیستم به دلیل این‌که چندین اینترفیس شبکه وجود دارد، برای این‌که برنامه دچار اشتباه نشود، آی‌پی سیستم اسکنر تحت فلگ ldap-server– به برنامه داده شده است.
- دو فلگ برای شناساندن سرور به برنامه وجود دارد : ldap-server-- و dns-server--

برای شناساندن آی‌پی اسکنر باید از یکی از این فلگ‌ها استفاده شود که تنها استفاده از ldap-server– کافی است و به این ترتیب همان آی‌پی برای سرور dns هم مورد استفاده قرار می‌گیرد.

- هنگام استفاده از ldap-server– دقت شود که حتما پورت ۱۳۸۹ به برنامه شناسانده شود تا دقت برنامه بالا رفته و تمامی موارد را تشخیص بدهد.
- به همین ترتیب برای سرور dns نیز حتما پورت ۵۳ تعیین شود چرا که بسیاری از سرورها اجازه اتصال به پورت dns غیر از پورت ۵۳ را نمی‌دهند.

پورت‌های هدف را می‌توانیم با استفاده از فلگ ports– به اسکنر تعریف کنیم. اگر این فلگ مورد استفاده قرار نگیرد برنامه پورت‌های پیش‌فرض خود را مورد استفاده قرار خواهد داد. استفاده از این فلگ می‌تواند به ۳ شکل صورت بگیرد:

- استفاده از یک پورت مثلا: ports=80-- ، در این صورت تنها این پورت مورد اسکن قرار خواهدگرفت.
- استفاده از چند پورت دلخواه مثلا: ports=80,443,8080– ، در این صورت این ۳ پورت مدنظر قرار خواهد گرفت.
- استفاده از بازه‌ای از پورت‌ها مثلا: ports=8000:9000-- در این صورت تعداد ۱۰۰۰ پورت از پورت ۸۰۰۰ تا پورت ۹۰۰۰ مورد اسکن قرار خواهد گرفت. اسکنر حداکثر ۱۰۲۴ پورت را قبول می‌کند.
- استفاده از پورت‌های پیش‌فرض مثلا: ports=top10-- یا ports=top100– ، در این صورت پورت‌های از قبل تعیین شده توسط خود برنامه که پورت‌های معمول وب هستند مورد استفاده قرار خواهد گرفت.

اگر فرضا بخواهیم یک وب‌سرور موجود در اینترنت را مورد بررسی قرار دهیم ابتدا باید آی‌پی آن را استخراج کنیم. ابزارهای مختلفی برای این منظور موجود است. پس از اطلاع از آی‌پی هدف و اگر فرضا بخواهیم ۱۰ پورت مهم را بر روی این سرور اسکن کنیم دستور اجرایی به صورت زیر خواهد بود:

```
log4jScanner.exe scan --ip=142.250.179.142 --ports=top10 --ldap-
server=2.187.250.124:1389
```

- این دستور وب‌سایت google.com را که آی‌پی آن ۱۴۲.۲۵۰.۱۷۹.۱۴۲ است برای ۱۰ پورت وب معروف مورد اسکن قرار خواهد داد.
- دقت شود که آی‌پی سرور هم متناسب با نوع اسکن تغییر کرده و آی‌پی خارجی سیستم مورد استفاده قرار گرفته است. اگر این آی‌پی به صورت صحیح تعیین نشود ابزار قادر به تشخیص موارد آسیب‌پذیر نخواهد بود.

دستورات ذکر شده در بالا بر روی سیستم عامل ویندوز اجرا شده است و بر روی سیستم عامل لینوکس هم این دستورات یکسان بوده و تنها فراخوانی فایل اجرایی متفاوت است. به عنوان مثال اگر همان دستور بالا را بخواهیم بر روی سیستم لینوکس به کار ببریم پس از اجرای ترمینال و ورود به پوشه حاوی فایل اجرایی دستور زیر را اجرا می‌کنیم:

```
sudo ./log4jScanner scan --ip=142.250.179.142 --ports=top10 --ldap-
server=2.187.250.124:1389
```

در انتها یادآور می‌شود که فلگ‌های دیگری نیز برای دیگر تنظیمات دلخواه وجود دارند که با استفاده از دستور زیر می‌توان به آن‌ها دسترسی پیدا کرد:

```
log4jScanner.exe scan --help
```