آموزش راه اندازی OpenVAS در کالی لینوکس (نسخه PDF)

در این آموزش قصـد داریم تا نحوه راه انـدازی و در نهایت اسـتفاده از OpenVAS در لینوکس کـالی را به شـما آموزش دهیم. همانطور که میدانیـد و شاید هم ندانید! OpenVAS که مختصر شده Open Vulnerability Assessment Systerm میباشد، یک اسـکنر آسیب پذیری قوی است که هزاران فیلتر برای چک و بررسی آسیب پذیری را در بر میگیرد. استفاده از این ابزار کاملا رایگان و بصورت اپن سورس است.

راه اندازی اولیه OpenVAS

OpenVAS یـک فریـم ورک بسـیار قدرتمنـد است و برای اسـتفاده از آن نیازمنـد انجـام برخی پیش نیازهـا هسـتیم. اولین مرحله اجرای اسکریپت Openvas-setup برای نصب پلاگین ها مربوطه و اسـتارت سرویس های مختلفی است که OpenVAS بر اساس آن ها کار میکند. در ادامه کار هنگامی که از شما پسورد خواسته شد، یک کلمه عبور قوی برای یوزر ادمین خود ایجاد کنید.

```
root@kali:~# openvas-setup
/varlib/openvas/private/CA created
/var/lib/openvas/CA created

[i] this script synchronizes an NVT collection with the 'openVAS NVT Feed'.
…
Stopping OpenVAS manager: openvasmd.
Stopping OpenVAS scanner:   openvassd.
Loading the openvas plugins…
Base gpgme-message: setting GnuPG homedir to '/etc/openvas/gnupg'
Base gpfme-,essage: using OpenPGP engine version '1.4.12'
All plugins loaded
Starting OpenVAS scanner:   openvassd.
Starting OpenVAS manager: openvasmd.
Restarting OpenVAS Administrator: openvasad.
Restaring Greenbone Security Assistant: gsad.
Enter password:
Ad main:MESSAGE:810:2015-06-17 14h03.20 EDT: No rules file provided, the new user will have no restrictions.
Ad main:MESSAGE:810:2015-06-17 14h03.20  EDT: User admin has been successfully created.
```

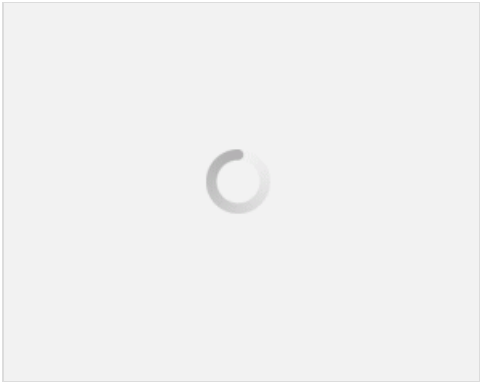
اگر اجرای این مرحله کمی! بیشتر از آن چیزی که اینجا نشان دادیم، طول کشید، تعجب نکنید.در گام بعد باید یک یوزر برای لاگین کردن به openvas بسازیم. این کار را با اسکریپت openvas-adduser انجام میدهیم.

```
root@kali:~# openvas-adduser
using /var/tmp as a temprory file holder.



Add a new openvassd user



Login: root
```

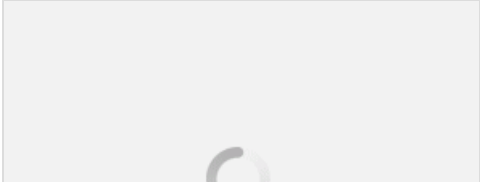
```
Authentication (pass/cert) [pass] : pass
Login password:
Login password (again) :

User rules

Openvassd has a rules system which allows you to restrict the hosts that root has the right to test.
For instance, you may want him to be able to scan his own host only.


Please see the openvas-adduser(8) man page for the rules syntax.

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)

Login  : root
Password :************


Rules  :
Is that ok? (y/n)[y] y
User added.
```

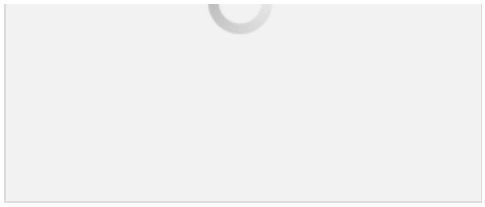
بـا یوزری که ایجاد کردیم، میتوانیم به Greenbnone Security Desktop دتسرسـی داشـته باشیم و با حساب کاربری که ایجاد کردیم، به آن لاگین کنیم.

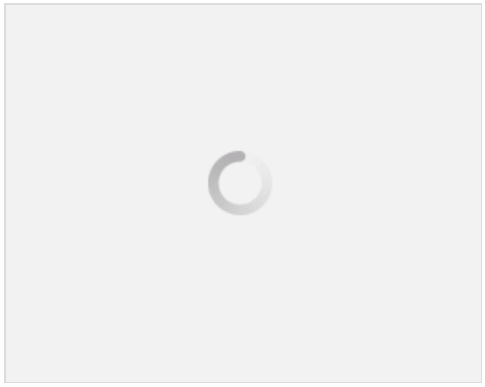
```
root@kali:~# gsd
```



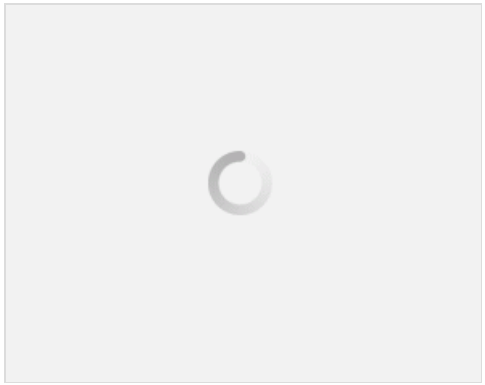
پس از لاـگین کردن، میتوانیـد اینترفیس Green Security Desktop را معرفی، اهـداف خود را کانفیـگ، task هـای مختلف ایجاد و نتایج اسکن آسیب پذیری را مدیریت کنید.



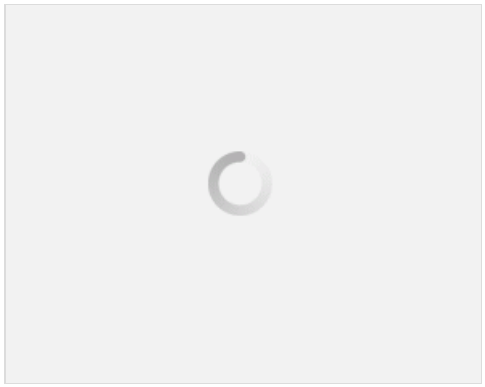




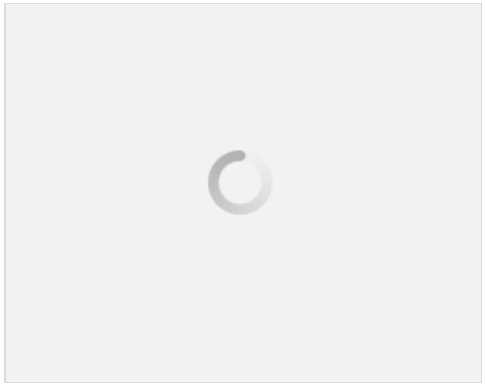
قبل از آن که اولین اسـکن آسـیب پذیری خود را با OpenVAS اجرا کنیم، نیاز داریم تا هـدف خود را معرفی کنیم. هـدف میتواند هم یک آدرس IP تنها باشد و هم میتواند محدوده ای از هاست ها را در بر بگیرد.

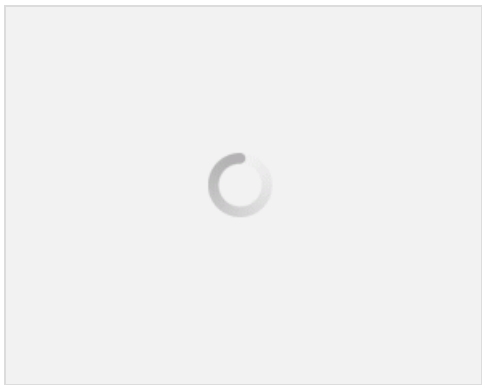


با وجود یک هدف کانفیگ شده، میتوانیم با استفاده از یکی از scan config های از پیش ساخته شده، یک scan task جدید ایجاد کنیم.

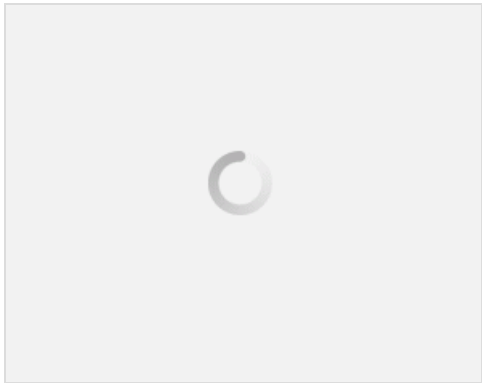


Task جدید بصورت خودکار شـروع بکار نمیکند، بنابراین باید بصورت دستی task مان را اجرا کنیم و منتظر بمانیم تا اسـکن آسیب پذیری به اتمام برسد. بسته به منابع موجود در سیستم شما، اسکن اسیب پذیری میتواند زمان زیادی را برای تکمیل خود صرف کند.





وقتی که اسکن به اتمام رسید، گزارش اسکن را میتوانید در زیر تب report مشاهده کنید. از آنجایی که اسکن اول ما بدون اعتبارات کاربری انجام شـد، تعـداد آسـیب پـذیری های یافت شـده بسـیار کم میباشد. علت این موضوع این است که برای نرم افزارهای موجود در هدف کوئری ارسال نشده است و یا آن که دیگر آسیب پذیری ها به احراز هویت نیاز داشتند.



سربلند و مانا باشید.

نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

حامد

درود ، دوست عزیز آموزش کامل تر از این موجود هست ؟؟؟

احسان امجدی

ممنون. بله این فقط آمورش مقدماتی برای راه اندازی بود... قطعا اموزش های کامل تری هم وجود داره...

حامد

اگه منبعی سراغ دارین معرفی کنید ممنون می شم اگه فارسی هم باشه خیلی عالی میشه

مطلب اصلی