تهیه و تنظیم : آریا صادقی

ایمیل : aryasadeghy@gmail.com

آی دی تلگرام : @aryasadeghy

مقدمه:

یکی از خسته کننده ترین قسمت در هکینگ و یا امنیت ، پی بردن و کشف کردن باگ بر روي نقطه اي خاص است. ولی این بخش براي دوستانی که در "هک قانونمند" مشغول به کارند بسیار کاربردي است. پس سعی کنید پس از این بخش دنبال مطالب قویتر و بروزتر در این بخش باشید.

شناسایی آسیپ پذیري براي دوستانی که در این عرصه کار می کنند مشق شب محسوب می شود. پس این فصل را جدي بگیرید و سعی کنید در آن بروز باشید و وقتی شما آسیبی را بشناسید می توانید راحت تر مشکل خود را حل کنید. در این بخش 2 ابزار کاربردي به نام هاي Nessusو vega scanner را به شما معرفی میکنم و در پست های بعدی به آ«وزش آن ها نیز خواهیم پرداخت .

Vulnerability چیست؟

در فارسی به صورت "نقطه ضعف" یا "حفره" یا "آسیب پذیري" ترجمه شده است و تعریف رایج آن عبارت است از : هرگونه ضعف نرم افزاري که قابل سوء استفاده باشد.

Vulnerability Scanner چیست؟

ابزاري است که به کمک آن می شود کامپیوترهاي شبکه را از نظر وجود حفره هاي امنیتی تست کرد.VulnerabilityScanner این کار را به صورت اتوماتیک یا نیم اتوماتیک انجام می دهد .

False Positive چیست؟

یعنی مواردي که اسکنر تشخیص میدهد که یک vul در سیستم است در حالیکه چنین نیست. این مورد خیلی وقتها پیش می اید و هیچ هم عجیب نیست. پس وقتی Vul Scanner یک Vul رو تشخیص می دهد، زیاد هم لذت نبرید!

آسیب پذیري ها عبارتند از:

1- Linux vulnerabilities

2- Windows vulnerabilities

3- Local security checks

4- Network service vulnerabilities

Nessus :

آموزش نصب Nessus :

لینک دانلود اما اینم بگم باید با یه vpn دانلود کنید برای کشور بستس دی:

nessus: http://www.tenable.com/products/nessus/select-your-operating-system

بعد از دانلود برا اساس نوع سیستم عامل اون رو به این صورت نصب و به اجرا در بیاورید

۱– ابتدا به آن دایرکتوری که فایل شما در آن است بروید و در ترمینال دستور زیر را وارد کنید

sudo dpkg -i Nessus*.deb

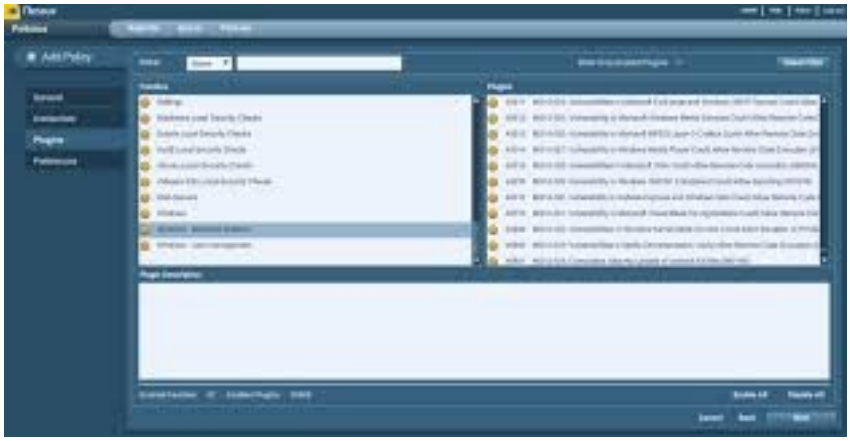
و اون رو اینجوری اجرا کنید .

sudo /etc/init.d/nessusd start

خب حالا مرورگر رو باز کنید و آدرس زیر رو تایپ کنید

https://localhost:8834

محیط آن را میتوانید در عکس زیر مشاهده کنید.



Vega scanner :

آموزش نصب :

برای نصب به آدرس زیر برید و دانلودش کنید:

https://subgraph.com/vega/download

پس از دانلود اون رو از از حالت فشرده خارج کنید و با ترمینال به دایرکتوری که فایل ها آن جاست بروید و با دستور زیر آن را اجرا

کنید.

sudo ./Vega

امیدوارم که لذت کافی رو برده باشید .