privacy

علشان اعمل penetration testing او حتى attacking على حد لازم أكون مخفى بالنسبه للشخص وان ميتحددليش هويه او اسمح انه يعملى tracing او يعرف موقعى او حتى امنع نشر بيانات عنى علشان متستخدمش ضدى من قبل ال ISP اللى انا تابع ليه او حتى من الجهات الحكوميه، لان اى مستخدم للويب بيكون ممكن جلب كل المعلومات اللى تخصه وتخص نشاطه على الانترنت بسهوله.

من هنا وعلشان يبقا في more privacy في استخدام الانترنت طلعت تقنيات زى ال proxy وال proxychain وال VPN وال Tor وغيرهم اللى بيخلوا الاتصال يمر باكتر من مرحله بحيث يكون مصدر الاتصال غير محدد او على الأقل صعب جدا تحديده.

في الأول ال proxy دا هو عباره عن وسيط بين المستخدم والانترنت، بستخدمه فانه ينفذ الأوامر عنى، يعنى انا مثلا علمت request لصفحه معينه، فبيتم ارسال الطلب دا منى لل proxy server ويكون قدام الانترنت هو اللى طلبه، نفس الفكره لل VPN.

بس بيكون موضوع استخدام ال proxy وال VPN مش كفايه لان بيكون مش من الصعب تحديده وكمان مبيخفيش معلومات ال DNS بتاعتى، فعلشان كدا ظهر تقنيات زى ال proxychain وال socks وال whonix.

Whonix®

هو عباره عن منظمه بتدعم حرية استخدام الانترنت من غير مراقبه على استخدام الأشخاص من قبل مزودين الخدمه او الحكومات، فبيتم استخدام ال tor الخاص بيهم ودا اللى بيخلى الاتصال يمر بمراحل كتير بحيث انه يكون من الصعب جدا تحدديه وكمان بيتم تشفير الداتا الخاصه ببرتكول http بحيث ان لو تم الحصول على الداتا بتاع التصفح بتاعتى تكون مشفره.

ال whonix هو عباره عن OS في واحد منه عباره عن terminals commands وواحد تانى عباره عن GUI، بيتم تنصيبه على ال OS الخاص بيا عن طريق virtual machine.

طيب ازاى انشأ اتصال عن طريق ال whonix Tor ؟

على ال whonix GUI:

- اول حاجه اشغل ال Tor واتأكد انه شغال عن طريق أداة ال whonix check
- بعدبن بشغل أداة reload tor بيفتحلى ال terminals وبيقلى ان ال status بتاعته active
- بستخدم امر sudo ifconfig علشان اعرف بيانات ال DNS وال IP وال netmask اللى هستخدمهم في الاتصال على ال kali

على ال Kali:

- اتأكد اول حاجه انى مخلى ال kali متصل على ال whonix network card في اعدادت ال network الخاصه بال kali على ال VM
- اقطع الاتصال بالشبكه اما manually او عن طريق امر ifdown eth0
- بعد كدا بغير الكونفيجريشن بتاع الشبكه من automatic ل manually واحط ال ip وال netmask وال DNS اللى جبتهم من whonix
- ال IP اللى جبته من ال whonix هو ال gateway الخاص بالشبكه فلما احط ال IP في الكونفيجريشن على ال kali بزود على ال IP واحد
- بعد كدا اروح اعمل check من على موقع dnsleaktest.com