**مركز الحماية السيبرانية للكشف و التحليل الرقمي**

**SOC Center**

في مجال الأمن السيبراني، قد يكون تطبيق وتنفيذ مفاهيم الأمان مهمة شاقة في حالة عدم توفر بنية تحتية عملية وآمنة لتنفيذ هذه الأنشطة.

لقد اقتربت من هذا المشروع مع أخذ ذلك في الاعتبار. يستعرض هذا االمشروع التطبيقي عملية تكوين البنية التحتية لتكنولوجيا المعلومات وتحسينها وتأمينها. على الرغم من أن هذا سيكون على نطاق صغير نسبيًا، إلا أننا سنكون قادرين على تطبيق المعرفة المكتسبة في البنية التحتية للمؤسسات/الواسعة النطاق في العالم الحقيقي.

**محتوى**

* بناء جهاز الكمبيوتر المضيف
* تثبيت VMware Workstation كمشرف على الأجهزة الافتراضية
* تكوين جدار الحماية pfSense لتقسيم الشبكة وأمنها
* تكوين Security Onion باعتباره حل IDS ومراقبة الأمان وإدارة السجل الشامل
* تكوين Kali Linux كآلة هجوم
* تكوين خادم Windows كوحدة تحكم بالمجال
* تكوين أجهزة سطح المكتب ويندوز
* تكوين سبلانك
* أجهزة Ubuntu /Metasploitable جميعها عبارة عن أجهزة Linux محتملة يمكن إضافتها إلى الشبكة لأغراض الاستغلال أو الكشف أو المراقبة*.*

Topology

