Cybersecurity Lab Documentation

Created	@August 6, 2025 9:33 PM
Status	Not started

🧪 توثيق إعداد معمل الأمن السيبراني (Cybersecurity Lab Documentation)

🗂️ نظرة عامة

تم إعداد معمل يحتوي على بيئة هجومية ودفاعية مكونة من 12-14 جهازًا (6-7 أجهزة دفاعية و6-7 أجهزة هجومية)، بهدف إجراء اختبارات الاختراق، التحليل الأمني، واختبار تقنيات الكشف عن التهديدات والاستجابة لها.

🖥️ مكونات المعمل

🔐 الأجهزة الدفاعية (Defensive Machines)

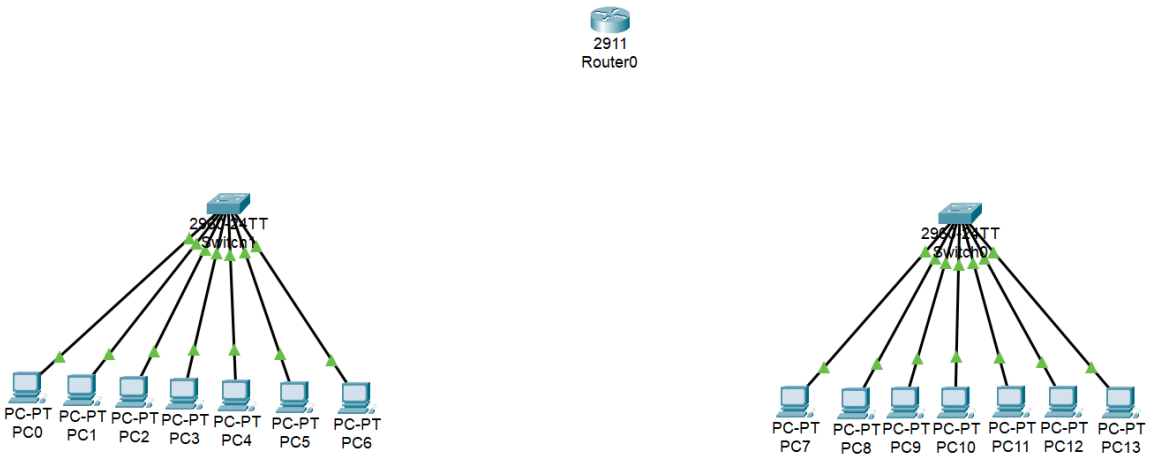
- **العدد**: 6-7 أجهزة
- **الاتصال الشبكي**: مرتبطة عبر Switch-1

- content also GNS3
- **نظام التشغيل الأساسي**:
  - VMware
- **أنظمة الضيوف (VMs)**:
  - **Metasploitable 2**: كنظام هدف لاختبار أدوات التحليل والكشف.
  - **Snort**: نظام كشف التسللات (IDS) في النظام الأساسي (host OS)
  - **Kali Linux**: يحتوي على الأدوات التالية:
    - **Nessus**: ماسح ثغرات احترافي
    - **OpenVAS**: نظام فحص ثغرات مفتوح المصدر
    - **OpenCTI**: منصة استخبارات تهديدات مفتوحة المصدر
- **أحد الأجهزة الدفاعية يحتوي أيضًا على**:
  - **ELK Stack (Elasticsearch - Logstash - Kibana)**: لتحليل السجلات وتصور البيانات الأمنية

🗡️ الأجهزة الهجومية (Offensive Machines)

- **العدد**: 6-7 أجهزة
- **الاتصال الشبكي**: مرتبطة عبر Switch-2
- content also GNS3
- **نظام التشغيل الأساسي**:
  - VMware
- **أنظمة (VMs)**:
  - **Kali Linux**: تستخدم لتنفيذ هجمات اختبارية على الأجهزة الدفاعية

🔌 هيكل الشبكة



⚙️ الأدوات والبرمجيات المستخدمة

الوصف	الأداة / النظام	القسم
نظام يحتوي ثغرات لاختبار أدوات الدفاع	Metasploitable 2	الدفاعي
بيئة تحليل أمنية	Kali Linux	الدفاعي
ماسح ثغرات احترافي	Nessus	الدفاعي
فاحص ثغرات مفتوح المصدر	OpenVAS	الدفاعي
منصة استخبارات تهديدات	OpenCTI	الدفاعي
نظام كشف التسللات	Snort	الدفاعي
تحليل السجلات والتصور	ELK Stack	الدفاعي
بيئة هجوم و Pentesting	Kali Linux	الهجومي

🎯 أهداف المعمل

- اختبار أدوات الدفاع مثل Snort وELK وOpenCTI ضد هجمات حقيقية.
- تنفيذ هجمات مثل مسح الشبكة، استغلال الثغرات، وتنفيذ هجمات MITM.
- مراقبة وتحليل الأنشطة الخبيثة باستخدام منصات كشف التسلل والتحليل.
- دراسة الاستجابة للهجمات وتحليل السجلات الناتجة.

📝 ملاحظات إضافية

- تم عزل الشبكتين (الهجومية والدفاعية) عبر استخدام switches مختلفين لتقليل التداخل.
- يتم تخزين وتحليل السجلات على جهاز واحد فقط (ELK).