### **7.2.1 Recursos gratuitos**

**7.2.1.6**

[**http://www.flu-project.com/2014/03/ejecutando-nmap-desde-python.html**](http://www.flu-project.com/2014/03/ejecutando-nmap-desde-python.html)

Aquí podemos encontrar una guía para implementar Nmap con Phyton.

**7.2.1.7**

Nmap se desarrolla en entornos gratuitos basados en los sistemas operativos GNU/Linux, Solaris, BSD y Mac OS X.

Unix: **https://es.wikipedia.org/wiki/Unix**

### **7.2.2 Recursos no gratuitos**

**7.2.2.1**

[**https://lunarline.com/vulnerability-scan-converter**](https://lunarline.com/vulnerability-scan-converter)

LunarLine Vulnerability Scan Converter VSC es una herramienta complementaria a Nmap que convierte instantáneamente archivos desde el escáner de vulnerabilidades en una hoja de Excel consolidada en un formato legible.

Después de procesar los datos, se compila la información de su vulnerabilidad en un solo libro de Excel. El usuario solo tendrá acceso a las hojas de cálculo con información sobre cada instancia de cada vulnerabilidad encontrada aunque también hay hojas de trabajo que proporcionan información adicional de vulnerabilidad, incluyendo el nivel de riesgo que plantea la vulnerabilidad, así como una lista de hosts donde se encontró una vulnerabilidad determinada. También se organizan los libros de hojas de cálculo en formatos comunes de evaluación, tales como NIST, DIACAP, e incluso FedRAMP. También tendrá acceso a una hoja de cálculo que proporciona información sobre todos los puertos que escanea Nmap.

Es una herramienta cuya licencia es de pago pero también tiene una versión gratuita de prueba. El precio de la licencia sería de 999$.

**7.2.2.2**

Nmap también se desarrolla en entornos de pago basados en los sistemas operativos Microsoft Windows y AmigaOS, por lo que esta herramienta es multisistema.

Microsoft Windows: [**https://www.microsoft.com/es-es/windows/**](https://www.microsoft.com/es-es/windows/)

AmigaOS: **http://www.amigaos.net/**