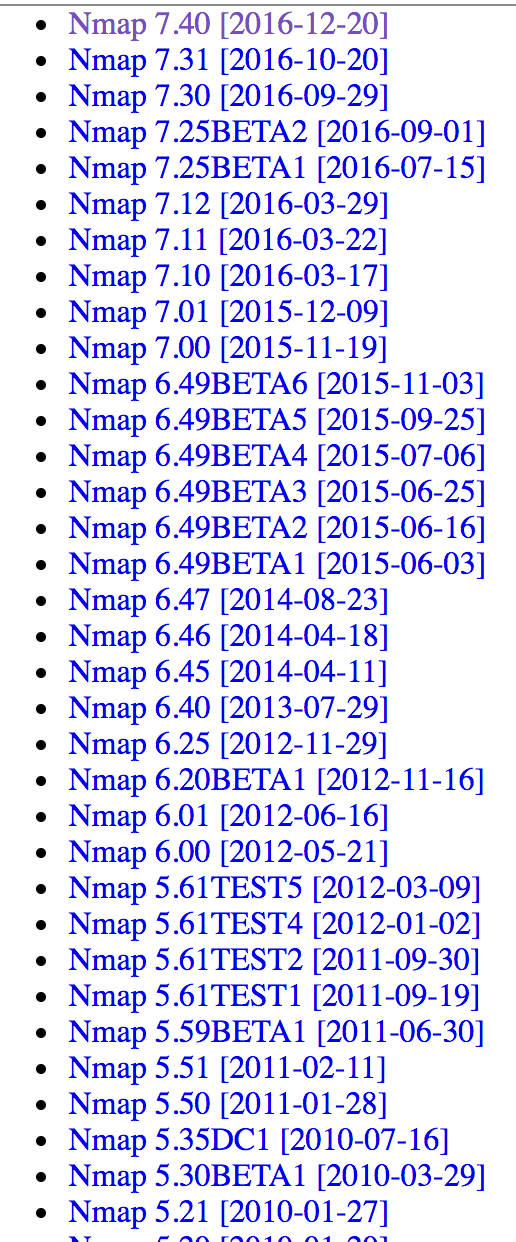
## 4.1 Evaluación de los criterios para la tecnología Nmap

|  |  |
| --- | --- |
| CRITERIOS | EVALUACIONES |
| Criterio A.1: Madurez y versiones | Dispone de muchas versiones y formatos ya que esta disponible para varios sistemas operativos. Algunas son Nmap7.40, Nmap 7.31, Nmap 7.30 \* |
| Criterio A.2: Coste | 0 € |
| Criterio A.3: Desarrollador | Gordon Lyon (más conocido por su alias Fyodor Vaskovich) |
| Criterio A.4: Flexibilidad de idiomas | Inglés |
| Criterio A.5: Lenguajes de programación | C, C++, Phyton, Java y Perl |
| Criterio A.6: Instalación | Fácil, Nmap ofrece una guía de ayuda para la instalación |
| Criterio A.7: Popularidad | Elevada al ser una herramienta gratuita, con tantas versiones y de las más competitivas |
| Criterio A.8: Competitividad | Aparece entre las 10 mejores herramientas de seguridad en distintos artículos. \* |
| Criterio B.1: Respaldo | Hay disponible un montón de libros, foros, artículos y video tutoriales donde se ofrece ayuda. La propia página de Nmap muestra una guía |
| Criterio B.2: Garantía | Alta |
| Criterio B.3: Soporte | Si |
| Criterio B.4: Cantidad de información | Proporciona una gran variedad de información. \* |
| Criterio C.1: Configuración | Fácil, limitada y extensa |
| Criterio C.2: Interfaz intuitiva | Si |
| Criterio C.3: Dificultad de uso | Si |
| Criterio C.4: Exportación de resultados | HTML,XML, NMAP, grepeable y script kiddies |
|  |  |
|  |  |
| Criterio C.5: Integración | Alta, con herramientas como Lunarline, Phyton… Tiene 3 herramientas integradas: NCAT, NDIFF y NPING |
| Criterio C.6: Plataformas disponibles | Linux, Windows Microsoft, Mac os x, FreeDSD, OpenBSD, NetBSD,  Sun Solaris, Amiga, HP-UX y AIX |
| Criterio C.7: Complejidad | Media |
| Criterio C.8: Tiempo ejecución | Dependerá del método de escaneo: ping, paquetes timestamp, paquetes netmask request, sólo el paquete ACK dirigiéndolo a un puerto determinado, paquetes SYN al puerto 20, paquetes UDP al puerto 20 |
| Criterio C.9: Calidad informe | Alta |
| Criterio D.1: XSS (Cross-site Scripting) | No |
| Criterio D.2: Rechazo de la inyección / respuesta de cabecera CRLF / HTTP | No |
| Criterio D.3: Inclusiones de archivos remotos | No |
| Criterio D.4: Mal uso de los puertos SSL y TSL para los pagos | Si |
| Criterio D.5: Mal uso de los puertos HTTPS | Si |
| Criterio D.6: Errores de desarrollo | Si |
| Criterio D.7: Errores de diseño | Si |

-Criterio A.1: Madurez y versiones: Más versiones:



-Criterio A.8: Competitividad: Esta fuente nos muestra las 8 mejores herramientas de seguridad y hacking, entre las que aparece Nmap.

[**http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/**](http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/)

-Criterio B.4: Cantidad de información:

* Descubrimiento de [servidores](https://es.wikipedia.org/wiki/Servidores): Identifica computadoras en una red, por ejemplo listando aquellas que responden [ping](https://es.wikipedia.org/wiki/Ping).
* Identifica [puertos](https://es.wikipedia.org/wiki/Puerto_(computaci%C3%B3n)) abiertos en una [computadora](https://es.wikipedia.org/wiki/Computadora) objetivo.
* Determina qué servicios está ejecutando la misma.
* Determinar qué [sistema operativo](https://es.wikipedia.org/wiki/Sistema_operativo) y versión utiliza dicha computadora, (esta técnica es también conocida como [*fingerprinting*](https://es.wikipedia.org/wiki/Fingerprinting)).
* Obtiene algunas características del hardware de red de la máquina objeto de la prueba.