Reporte de vulnerabilidades

Ejemplo

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
80	HTTP	Apache 2.4.7	CVE-2019-0211	Escalación de privilegios en Apache HTTP Server.	Link a CVE
443	HTTPS	OpenSSL 1.0.1f	CVE-2014-0160	Heartbleed: Exposición de memoria del servidor.	Link a CVE
22	SSH	OpenSSH 6.6.1p1	CVE-2015-5600	Ataque de fuerza bruta por defecto débil.	Link a CVE

Se han encontrado estas 5 vulnerabilidades dentro de Bee Box usando el escaneo Nmap
Comando usado
nmap -sV –script=vuln 10.0.2.15 (IP de Bee Box)
nmap -p 22,80,443 -T5 -v -sV --script=vuln 10.0.2.15

Puerto	servicio	Version	Vulnerabilidad	Descripcion	Referencia
80	apache	2.2.8	CVE-2011-3607	Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.	Enlace
80	apache	2.2.8	CVE-2012-0031	scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by	Enlace

				modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.	
80	apache	2.2.8	CVE-2007-6750	The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod_reqtimeout module in versions before 2.2.15.	Enlace
80	apache	2.2.8	CVE-2010-1623	Memory leak in the apr_brigade_split_line function in buckets/apr_brigade.c in the Apache Portable Runtime Utility library (aka APR-util) before 1.3.10, as used in the mod_reqtimeout module in the Apache HTTP Server and other software, allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors related to the destruction of an APR bucket.	Enlace
80	apache	2.2.8	CVE-2013-5704	The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."	Enlace