Disponibilitat de serveis amb Nmap

Disponibilitat de serveis amb Nmap

Identificar i analitzar la disponibilitat de serveis o servidors, ports oberts i versions de sistemes operatius que els suporten, suposa la informació base per a l'estudi de les innumerables vulnerabilitats dels sistemes en xarxa. D'aquest mode es podran prendre mesures front a aquests punts febles dels nostres sistemes.

Nmap és una ferramenta de codi obert per a l'exploració de xarxa i auditoria de seguretat. Utilitza paquets IP per a determinar quins equips es troben disponibles a la xarxa, quins serveis ofereixen i mitjançant quines aplicacions (nom i versió de l'aplicació), quins sistemes operatius (i les seues versions) executen, quins tipus filtrat de paquets i tallafocs estan utilitzant, així com altres característiques.

Escaneig de ports amb Nmap

1. Instal·la Nmap a Rocky Linux des dels repositoris
2. Una vegada fet lo anterior, realitza un escaneig ràpid i sense opcions a `http://scanme.nmap.org`
3. Mostra els resultats i identifica a quin servei pertany cada port
4. Fes un nou escaneig i utilitza les opcions necessàries per tal d'identificar quin software es fa servir per al DNS i quin per al servidor Web. A més, identifica quina versió de eixe servidor web s'està utilitzant i sobre quin sistema operatiu. Adjunta una captura de pantalla a on senyales estos paràmetres.