Knife Tool Box

Rapport de l'outil Knife Tool Box

Hôte testé : 192.168.88.0/24

Vulnérabilités détectées :

Découverte de réseau : 192.168.88.1, 192.168.88.132, 192.168.88.136, 192.168.88.254 Ports ouverts : Port: 135, Service: msrpc Port: 139, Service: netbios-ssn Port: 445, Service: microsoft-ds Port: 5357, Service: wsdapi Port: 22, Service: ssh Port: 21, Service: ftp Port: 22, Service: ssh Port: 23, Service: telnet Port: 25, Service: smtp Port: 53, Service: domain Port: 80, Service: http Port: 111, Service: rpcbind Port: 139, Service: netbios-ssn Port: 445, Service: microsoft-ds Port: 513, Service: login Port: 514, Service: shell Port: 2049, Service: nfs Port: 2121, Service: ccproxy-ftp Port: 3306, Service: mysql Port: 5432, Service: postgresql Port: 5900, Service: vnc Port: 6000, Service: X11 Port: 8009, Service: ajp13 Starting Nmap 7.95 (https://nmap.org) at 2024-05-04 21:34 Paris, Madrid (heure d'été) Nmap scan report for 192.168.88.132 Host is up (0.0012s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 9.6p1 Debian 4 (protocol 2.0) | vulners: | cpe:/a:openbsd:openssh:9.6p1: | CVE-2012-1577 7.5 https://vulners.com/cve/CVE-2012-1577 |_ CVE-2023-51767 3.5 https://vulners.com/cve/CVE-2023-51767 MAC Address: 00:0C:29:55:D1:E7 (VMware) Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 2.48 seconds Connexion NOK admin/switch Connexion NOK admin/password Connexion NOK mohaa/switch Connexion OK mohaa/password Connexion NOK root/switch Connexion NOK root/password

Ports ouverts :

Host: 192.168.88.1, Port: 135, Service: msrpc Host: 192.168.88.1, Port: 139, Service: netbios-ssn Host: 192.168.88.1, Port: 445, Service: microsoft-ds Host: 192.168.88.1, Port: 5357, Service: wsdapi Host: 192.168.88.132, Port: 22, Service: ssh Host: 192.168.88.136, Port: 21, Service: ftp Host: 192.168.88.136, Port: 22, Service: ssh Host: 192.168.88.136, Port: 23, Service: telnet Host: 192.168.88.136, Port: 25, Service: smtp Host: 192.168.88.136, Port: 53, Service: domain Host: 192.168.88.136, Port: 80, Service: http Host: 192.168.88.136, Port: 111, Service: rpcbind Host: 192.168.88.136, Port: 139, Service: netbios-ssn Host: 192.168.88.136, Port: 445, Service: microsoft-ds Host: 192.168.88.136, Port: 513, Service: login Host: 192.168.88.136, Port: 514, Service: shell Host: 192.168.88.136, Port: 2049, Service: nfs Host: 192.168.88.136, Port: 2121, Service: ccproxy-ftp Host: 192.168.88.136, Port: 3306, Service: mysql Host: 192.168.88.136, Port: 5432, Service: postgresql Host: 192.168.88.136, Port: 5900, Service: vnc Host: 192.168.88.136, Port: 6000, Service: X11 Host: 192.168.88.136, Port: 8009, Service: ajp13

Hosts découverts :

192.168.88.1, 192.168.88.132, 192.168.88.136, 192.168.88.254