Diário de bordo

|  |  |  |
| --- | --- | --- |
| Data: |  | |
| Dados de endereçamento do(s) alvo(s) | IP: 192.168.2.254  MAC Address: E8:B1:FC:80:FD:E0 (Intel Corporate) | |
|  | | |
| Dados coletados de Rede (Portas/serviços, topologia) | | Comando utilizado |
| PORT |STATE |SERVICE |VERSION  -----------|---------|-----------|------------------------------------------  21/tcp |open |ftp |vsftpd 2.0.8 or later  -----------|---------|-----------|-------------------------------------------  80/tcp |open |http | Apache httpd 2.4.10 ((Debian))  -----------|---------|-----------|-------------------------------------------  111/tcp |open |rpcbind | (RPC #100000)  -----------|---------|-----------|-----------------------------------------  200. open | | nmap -T4 -A -v 192.168.2.254 |
| Dados coletados de aplicação (SO, versões de serviços..) | | Comando utilizado |
| Device type: general purpose  Running: Linux 3.X|4.X  OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4  OS details: Linux 3.2 - 4.8  Uptime guess: 0.043 days (since Thu Sep 27 11:32:43 2018)  Network Distance: 1 hop  TCP Sequence Prediction: Difficulty=259 (Good luck!)  IP ID Sequence Generation: All zeros | | nmap -T4 -A -v 192.168.2.254 |
| Vulnerabilidades | | |
| Comando utilizado: nmap –script vuln 192.168.2.254  Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-27 12:53 UTC  Pre-scan script results:  | broadcast-avahi-dos:  | Discovered hosts:  | 224.0.0.251  | After NULL UDP avahi packet DoS (CVE-2011-1002).  |\_ Hosts are all up (not vulnerable).  Nmap scan report for 192.168.2.254  Host is up (0.12s latency).  Not shown: 997 closed ports  PORT STATE SERVICE  21/tcp open ftp  |\_sslv2-drown:  80/tcp open http  |\_http-csrf: Couldn't find any CSRF vulnerabilities.  |\_http-dombased-xss: Couldn't find any DOM based XSS.  |\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  111/tcp open rpcbind  MAC Address: E8:B1:FC:80:FD:E0 (Intel Corporate) | | |
| Exploração | | |
|  | | |
| Outras informações úteis | | |
|  | | |