

Port	Service	Version	Vulnerability	Description	Reference
80	HTTP	Apache httpd 2.4.2((debian))	CVE-2018-1312	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent replay attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.	Link
139	NETBIOS-SSN	Samba smbd 4.6.2	No para esta versión		
443	SSL/HTTP	Apache httpd 2.4.62((debian))			
445	NETBIOS-SSN	Samba smbd 4.6.2	No para esta versión		

```
(kali@kali)-[~]
└─$ nmap -sV 192.168.1.63
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 13:33 EDT
Nmap scan report for 192.168.1.63
Host is up (0.00061s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.62 ((Debian))
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
443/tcp   open  ssl/http     Apache httpd 2.4.62 ((Debian))
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
MAC Address: 08:00:27:08:3C:56 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.83 seconds
```