

How To - Nmap vuln scanner script

Description

This document will show you how to do a vulnerability scan with Nmap. This script (vulners) already comes with the newer versions of Nmap.

Steps

1. Verify you have the vulners.nse script using the Linux terminal.

```
ls -la /usr/share/nmap/scripts/ | grep -e "vulners"
```

2. (Skip if installed) To install please visit this link for the guide.

<https://github.com/vulnersCom/nmap-vulners#installation>

3. Run the script.

```
sudo nmap -sV --script vulners [TARGET]
```

4. Example output.

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|     CVE-2010-4478  7.5  https://vulners.com/cve/CVE-2010-4478
|     CVE-2020-15778 6.8  https://vulners.com/cve/CVE-2020-15778
|     CVE-2017-15906 5.0  https://vulners.com/cve/CVE-2017-15906
|     CVE-2016-10708 5.0  https://vulners.com/cve/CVE-2016-10708
|     CVE-2010-4755  4.0  https://vulners.com/cve/CVE-2010-4755
|     CVE-2008-5161  2.6  https://vulners.com/cve/CVE-2008-5161
|_
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
```

Resources

- YouTube video: <https://www.youtube.com/watch?v=W0KRYkZpplw>
- Nmap vulners: <https://github.com/vulnersCom/nmap-vulners>