Vulnerability Scanning with nmap

NSE is like a digital library of scripts that we can use with Nmap to perform more advanced network scanning tasks beyond the basic port scanning and version detection. These scripts are written in the Lua programming language and can be used to automate various networking tasks like:

- Vulnerability detection
- Service enumeration
- Brute-force attacks
- Banner grabbing
- OS fingerprinting
- Backdoor identification
- Malware discovery
- And much more

One of the basic script scan we have used before also, is the scan with -sC flag. It is called the default script scan.

```
sudo nmap -sC IP
```

Next we have the vuln script scan,

So, nmap has a collection of scripts focus on identifying known vulnerabilities in the target system.

```
ls -l /usr/share/nmap/scripts/ | grep vuln
```

To perform a vuln script scan. We have to run

```
sudo nmap --script vuln IP
```

Moving on, we have vulners script, it uses the vulners.com online database to scan targets for the latest vulnerabilities. This script regularly updates its database to ensure you detect the most recent security flaws.

```
sudo nmap -sV --script vulners IP
```

At last, we have Vulnscan script scan. It is a comprehensive NSE script that utilizes several offline vulnerability databases, such as the National Vulnerability Database (NVD), Common Vulnerability and Exposures (CVE), and Open Vulnerability and Assessment Language (OVAL), to scan for vulnerabilities even when offline.

In order to use it, we first have to download the updated database from its github repo.

https://github.com/scipag/vulscan

```
git clone https://github.com/scipag/vulscan scipag_vulscan
sudo ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
```

To perform the scan, we have to run:

```
sudo nmap -sV --script vulscan/vulscan.nse IP
```
