Find Vulnerabilities using NMAP Scripts

Nmap Scripting Engine(NSE)

Developed for following reasons

1. Network Discovery
2. Classier version detection of a service
3. Backdoor Detection
4. Vulnerability Scanning

Nmap Script Categories

- Auth All sorts of authentication and user privilege scripts
- Brute set of scripts for performing brute force attacks to guess access credentials
- Discovery Scripts related to network ,service and host discovery
- Version OS,service and software detection scripts.

For listing all the available scripts in nmap

ls /usr/share/nmap/scripts

This will show multiple script.

Now make sure whatever command you are using it should be updated

For updation use
Sudo nmap –script-updatedb

Suppose you want to check particular script always use grep command.

Let suppose I want to use smb script (server message block)

ls /usr/share/nmap/scripts | grep smb
It will show all the scripts

Now suppose we want to check vulnerability in target operating system.

Type

Sudo nmap —script smb-vuln-ms17-010.nse target ip

This will show all the vulnerability.Now with the help of this vulnerability we can take access of our system.

Now for checking any directory we can use http

ls /usr/share/nmap/scripts/ | grep http

Sudo nmap –script http-enum.nse -p80 target ip

With the help of http grep we can find subdomains

Sudo nmap –script http-grep.nse -p80 target

How to crack any password?

We will use ftp script

ls /usr/share/nmap/scripts/ | grep ftp

This will list all the scripts
For password cracking

Use
nmap –script ftp-brute.nse -p21 targetip.