Nmap Scripting Engine

The Nmap Scripting Engine (NSE) is a powerful feature that allows interaction with services through Lua scripts. NSE scripts are divided into 14 categories, each serving different purposes:

- **auth**: Determines authentication credentials.
- **broadcast**: Uses broadcasting for host discovery.
- **brute**: Attempts login with brute-force credentials.
- **default**: Default scripts executed using the -sC option.
- **discovery**: Evaluates accessible services.
- **dos**: Checks for denial of service vulnerabilities.
- **exploit**: Tries to exploit known vulnerabilities.
- **external**: Uses external services for further processing.
- **fuzzer**: Identifies vulnerabilities and unexpected packet handling.
- **intrusive**: Contains intrusive scripts.
- **malware**: Checks for malware infection.
- **safe**: Defensive scripts that avoid intrusive actions.
- **version**: Extensions for service detection.
- **vuln**: Identifies specific vulnerabilities.

NSE Script Execution

There are different ways to execute NSE scripts in Nmap:

- **Default Scripts**:

```
sudo nmap <target> -sC
```

- **Specific Scripts Category**:

```
sudo nmap <target> --script <category>
```

- **Defined Scripts**:

```
sudo nmap <target> --script <script-name>,<script-name>,...
```

Example: Specifying Scripts

For example, let's use two defined scripts to analyze the SMTP port:

```
sudo nmap 10.129.2.28 -p 25 --script banner,smtp-commands
```

Example: Aggressive Scan

The -A option allows an aggressive scan with service and OS detection:

```
sudo nmap 10.129.2.28 -p 80 -A
```

Example: Vuln Category Scan

We can use the vuln category to assess vulnerabilities on HTTP port 80:

```
sudo nmap 10.129.2.28 -p 80 -sV --script vuln
```

The NSE scripts interact with the target services, providing valuable insights into their versions and potential vulnerabilities. More information about NSE scripts and categories can be found here.