Поиск уязвимостей через Nmap

Для начала нужно просканировать внешний IP на предмет открытых портов

```
nmap -sV -Pn -p- -T5 ваш ip
```

Далее ищем уязвимости ПО по найденным открытым портам из прошлой команды

```
nmap -sV -p 25,53,80,110,143,443,465,587,993,18231,44234 -T5 -Pn --script
vulners.nse ваш ip
```

Затем нужно проверить устойчивость к перебору паролей по 22 порту если будет открыт.

```
nmap --script ssh-brute -p 22 --script-args
userdb=users.lst,passdb=passwords.lst ваш ip
```

Так же проверить 21 порт

```
nmap -d --script ftp-brute -p 21 ваш ip
```

Если есть базы MySQL, проверяем анонимный доступ и подбор паролей

```
nmap -sV --script=mysql-empty-password ваше доменное имя
```

```
nmap --script mysql-brute -p 3306 ваше доменное имя
```

Проверка форм авторизации

```
nmap -p 80,443 --script http-auth-finder ваше доменное имя
```

Проверяем параметры найденых страниц

```
nmap -p-80,443 --script=http-form-brute --script-args=http-form-
brute.path=/login ваше доменное имя
```

Параметры

http-brute.hostname - имя хоста

http-form-brute.path - адрес страницы с формой или адрес с API

http-brute.method - тип метода, по умолчанию POST

http-form-brute.uservar - устанавливает имя переменной, которая отвечает за

username. Если не установлено, то скрипт возьмет имя поля из формы

http-form-brute.passvar - устанавливает имя переменной, которая отвечает за пароль. Если не установлено, то скрипт возьмет имя поля из формы

Параметры нужно перечислять через запятую после -script-args

Поиск скрытых папок и файлов

```
nmap -sV -p 80,443 -T5 --script http-enum ваше доменное имя
```

Для проверки уязвимостей sql баз нужно скачать sqlmap и python

```
C:\Users\i.kucherenko\Downloads\sqlmapproject-sqlmap-c5d7c54\sqlmap.py -u
https://ваш ip/index.php?id=1 --dbs -o random-agent
```

Проверка на XSS уязвимости Скачиваем XSStrike Далее через cmd устанавливаем

```
pip3 install pygame
```

```
pip3 install -r C:\Users\i.kucherenko\Downloads\XSStrike-
master\requirements.txt
```

Начинаем тестирование со сканирования всего сайта

```
python C:\Users\i.kucherenko\Downloads\XSStrike-master\xsstrike.py -u
"https://ваше доменное имя" --blind --crawl -l 100
```

Сканирование по конкретному параметру

```
python C:\Users\i.kucherenko\Downloads\XSStrike-master\xsstrike.py -u
"https://ваш ip/index.php?id=1" --blind
```

From:
https://wiki.fellk.ru/dokuwiki/ - **Игорь FellK**

Permanent link:
https://wiki.fellk.ru/dokuwiki/doku.php/poleznosti/vulnerability_search_nmap

Last update: **2024/06/24 13:03**