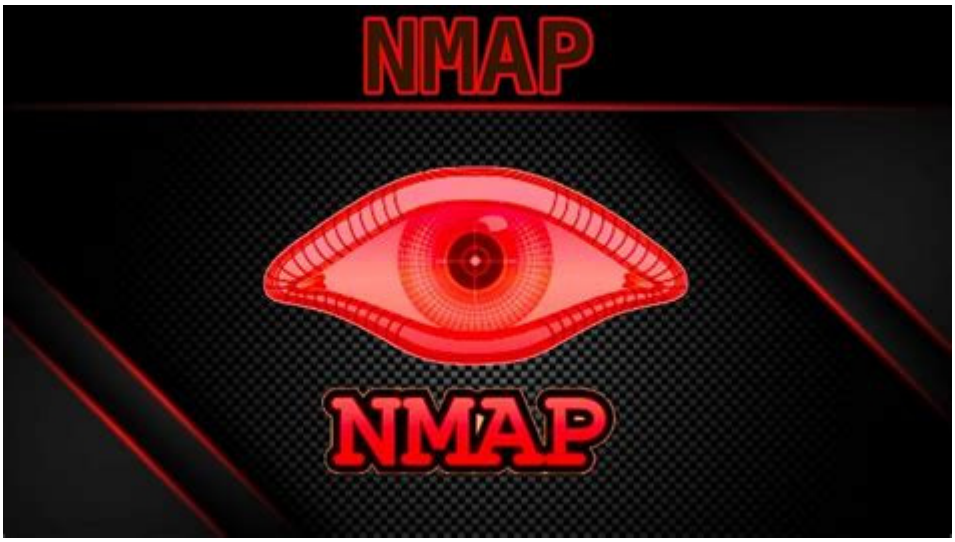
NMAP 3 часть – Telegraph

telegra.ph/NMAP-3-chast-05-07

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint May 7, 2024



Nmap Scripting Engine (NSE) — еще одна удобная функция Nmap. Она дает нам возможность создавать скрипты на Lua для взаимодействия с определенными сервисами. Всего существует 14 категорий, на которые можно разделить эти скрипты:

auth Определение учетных данных для аутентификации.

broadcast Скрипты, которые используются для обнаружения узлов сети с помощью широковещательной рассылки, могут быть автоматически добавлены к остальным сканированиям.

brute Выполняет сценарии, которые пытаются войти в соответствующую службу путем перебора учетных данных.

default Сценарии по умолчанию, выполняемые с помощью параметра -sC.

discovery Оценка доступных услуг.

dos Эти скрипты используются для проверки сервисов на наличие уязвимостей типа «отказ в обслуживании» и используются реже, так как это наносит вред сервисам.

exploit Эта категория скриптов пытается эксплуатировать известные уязвимости для сканируемого порта.

external Скрипты, использующие внешние сервисы для дальнейшей обработки.

fuzzer Скрипты для выявления уязвимостей и обработки неожиданных пакетов путем отправки различных полей, что может занять много времени.

intrusive Скрипты, которые могут негативно повлиять на целевую систему.

malware Проверяет, не заразило ли целевую систему какое-либо вредоносное ПО.

safe Безопасные сценарии, которые не осуществляют деструктивных действий.

version Расширение для обнаружения служб.

vuln Идентификация конкретных уязвимостей.

Сценарии по умолчанию:

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

Сценарии определенной категории:

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

Определенные скрипты:

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

Пример:

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

Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-16 23:21 CEST
Nmap scan report for 10.129.2.28
Host is up (0.050s latency).

PORT   STATE SERVICE
25/tcp open  smtp
|_banner: 220 inlane ESMTP Postfix (Ubuntu)
|_smtp-commands: inlane, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
MAC Address: DE:AD:00:00:BE:EF (Intel Corporate)
```

Мы видим, что можем распознать дистрибутив Linux Ubuntu с помощью сценария «banner». Скрипт «smtp-commands» показывает нам, какие команды мы можем использовать при взаимодействии с целевым SMTP-сервером. В этом примере такая информация может помочь нам найти существующих пользователей. Nmap также дает нам возможность сканировать нашу цель с помощью агрессивной опции (-A). При этом цель сканируется с использованием нескольких параметров, таких как обнаружение служб (-sV), обнаружение ОС (-O), трассировка (--traceroute) и сценарии NSE по умолчанию (-sC).

```
$ sudo nmap 10.129.2.28 -p 80 -A
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-17 01:38 CEST
Nmap scan report for 10.129.2.28
Host is up (0.012s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: WordPress 5.3.4
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: blog.inlanefreight.com
MAC Address: DE:AD:00:00:BE:EF (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 -
3.10 (96%), Linux 3.4 - 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%),
AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Synology DiskStation Manager
5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%),
Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   11.91 ms 10.129.2.28

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
```

С помощью параметра сканирования (-A) мы выяснили, какой веб-сервер (Apache 2.4.29) запущен в системе, какое веб-приложение (WordPress 5.3.4) используется, а также заголовок (blog.inlanefreight.com) веб-страницы. Кроме того, Nmap показывает, что это, скорее всего, операционная система Linux (96%).

Nmap предлагает нам шесть различных шаблонов синхронизации (-T <0-5>). Эти значения (0–5) определяют агрессивность нашего сканирования. Если сканирование слишком агрессивное, то системы безопасности могут заблокировать нас из-за создаваемого сетевого трафика. Шаблон синхронизации по умолчанию -T 3.

- -T 0 / -T paranoid
- -T 1 / -T sneaky
- -T 2 / -T polite
- -T 3 / -T normal
- -T 4 / -T aggressive
- -T 5 / -T insane