Внешний аудит безопасности корпоративных сетей

Лекция 12
Сетевой сканер Nmap II

Семён Новосёлов

Crypto Kantiana

БФУ имени И. Канта

2021

Скриптовый движок Nmap

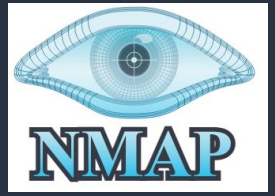
Список скриптов по категориям:

https://nmap.org/nsedoc/

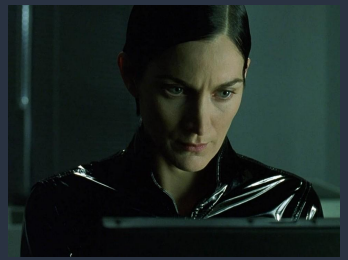
Использование:

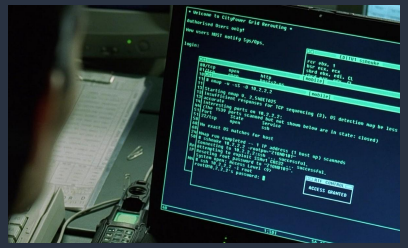
nmap -sV --script=http-sql-injection <target>

Свои скрипты запускаются таким же образом.



nmap.org





Nmap Scripting Engine (NSE)

Встроенный скриптовый движок на Lua.

Язык Lua

Строки

```
[[str1]], "str2",  'str3'
```

Циклы

```
while condition do
end

for i = start,finish,delta do
end

for k,v in pairs(tab) do
end
```

Функции

```
function f(a, b)
end
```

Условия

```
if condition then
elseif condition then
else
end
```

Комментарии

```
-- comment
--[[ Multiline
     comment ]]
```

Таблицы/массивы

```
a = {}
a = { a0 = 1, b0 = 2 }
a.a0 = 3

a = { ["hello"] = 200 }
a.hello

a = { "a", "b", "c", "d" }
print(a[2])          -- "b"
print(#a)            -- 4
```

Структура скрипта NSE

```
description = [[ описание скрипта ]]
author = {"Anonymous"}
license = "Same as Nmap--See
https://nmap.org/book/man-legal.html"
categories = {"intrusive"}
---
-- @usage
-- ...
-- @output
-- ...
-- @args ...
local stdnse = require 'stdnse'
local shortport = require 'shortport'

portrule = shortport.http

function action(host, port)
  local output = stdnse.output_table()
  output.some_result = 'found something'
  return output
end
```

документация

подключение библиотек (table, string, http, url, ...)

правило запуска (порт/сервис/хост)

выполняемое действие

Пример 1. Hello World

```
description = [[This is HELLO WORLD!!!]]
author = {"Anonymous"}
license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
categories = {"intrusive"}

local shortport = require 'shortport'
local stdnse = require 'stdnse'
local http = require 'http'

portrule = shortport.http

function action(host, port)
  local output = stdnse.output_table()
  local resp = http.get(host, port, "/hello/world?q=42")
  output.http_status =  resp.status
  output.http_headers = resp.rawheader
  return output
end
```

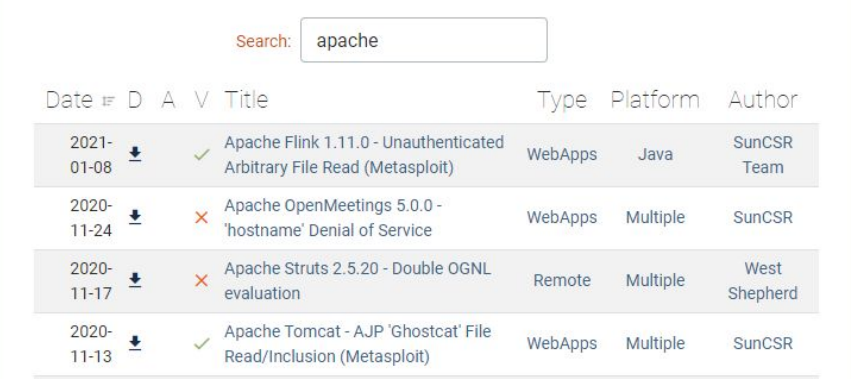
Пример 1. Результат выполнения

```
└─$ sudo nmap --script hello_world 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-20 18:01 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00022s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
| hello_world:
|   http_status: 404
|   http_headers:
|     Date: Thu, 20 May 2021 22:02:07 GMT
|     Server: Apache/2.2.8 (Ubuntu) DAV/2
|     Content-Length: 294
|     Connection: close
|     Content-Type: text/html; charset=iso-8859-1
|_
```

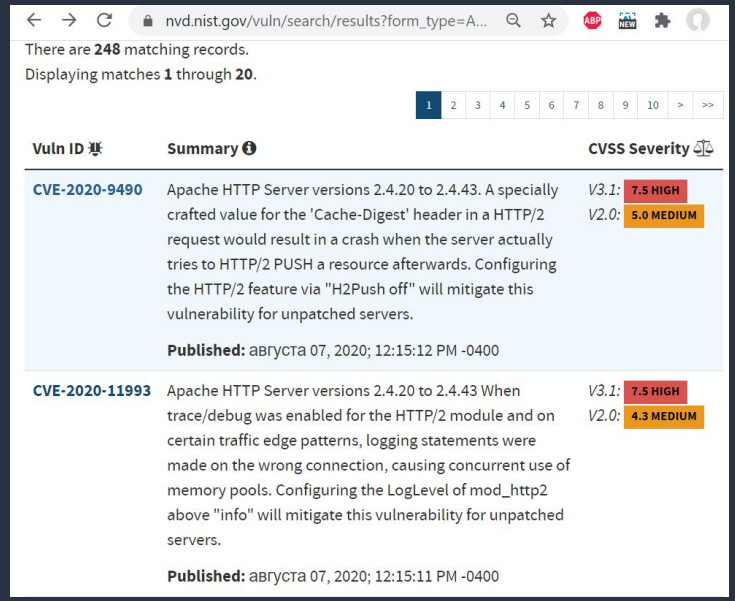
Пример 2. Поиск уязвимых серверов

Задача: найти сервера, уязвимые к заданным уязвимостям из базы CVE/NVD

Наиболее интересны уязвимости с эксплойтами:



exploit-db.com



Nmap позволяет просканировать массово сеть

Пример 2. Код

```
function action(host, port)
  local output = stdnse.output_table()
  local ver_rx = pcre.new("(?<major>[0-9]+)\\.(?<minor>[0-9]+)[\\.]?(?<patch>[0-9]*)", 0, "C")
  local res = {}
  local i,j,v = ver_rx:match(port.version.version, 0, 0)
  if (i) then
    major = tonumber(v.major)
    minor = tonumber(v.minor)
    patch = tonumber(v.patch)
    if (port.version.product=="Apache httpd") then
      if (major == 2 and minor == 2 and patch <= 34) or (major == 2 and minor == 4 and patch <= 27) then
        table.insert(res, {CVE="2017-9798", exploit="https://github.com/hannob/optionsbleed"})
      end
      -- ...
    end
  end
  if (#res > 0) then
    output.vulnerabilities = res
  end
  return output
end
```

Пример 2. Результат выполнения

```
└─$ sudo nmap -sV --script find_server 192.168.56.101 -n
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-20 20:57 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00065s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| find_server:
|   vulnerabilities:
|
|       CVE: 2017-9798
|_      exploit: https://github.com/hannob/optionsbleed
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

Литература и ссылки

- Gordon “Fyodor” Lyon. The Official Nmap Project Guide to Network Discovery and Security Scanning
  https://nmap.org/book/
- Документация по NSE:
  https://nmap.org/nsedoc/
- Ещё пример написания скрипта:
  https://xakep.ru/2016/02/25/pimp-my-nmap/
- Lua cheat sheet:
  https://devhints.io/lua