

Внешний аудит безопасности корпоративных сетей

Лекция 11 Сетевой сканер Nmap II



Семён Новосёлов

2022



БФУ имени
И. Канта

Скриптовый движок Nmap

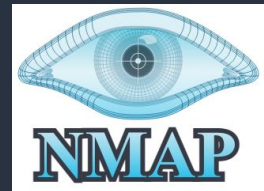
Список скриптов по категориям:

<https://nmap.org/nsedoc/>

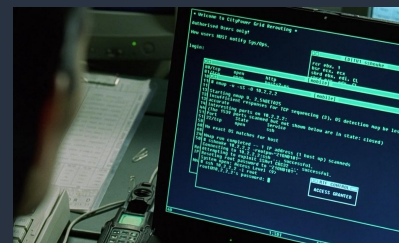
Использование:

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

Свои скрипты запускаются таким же образом.

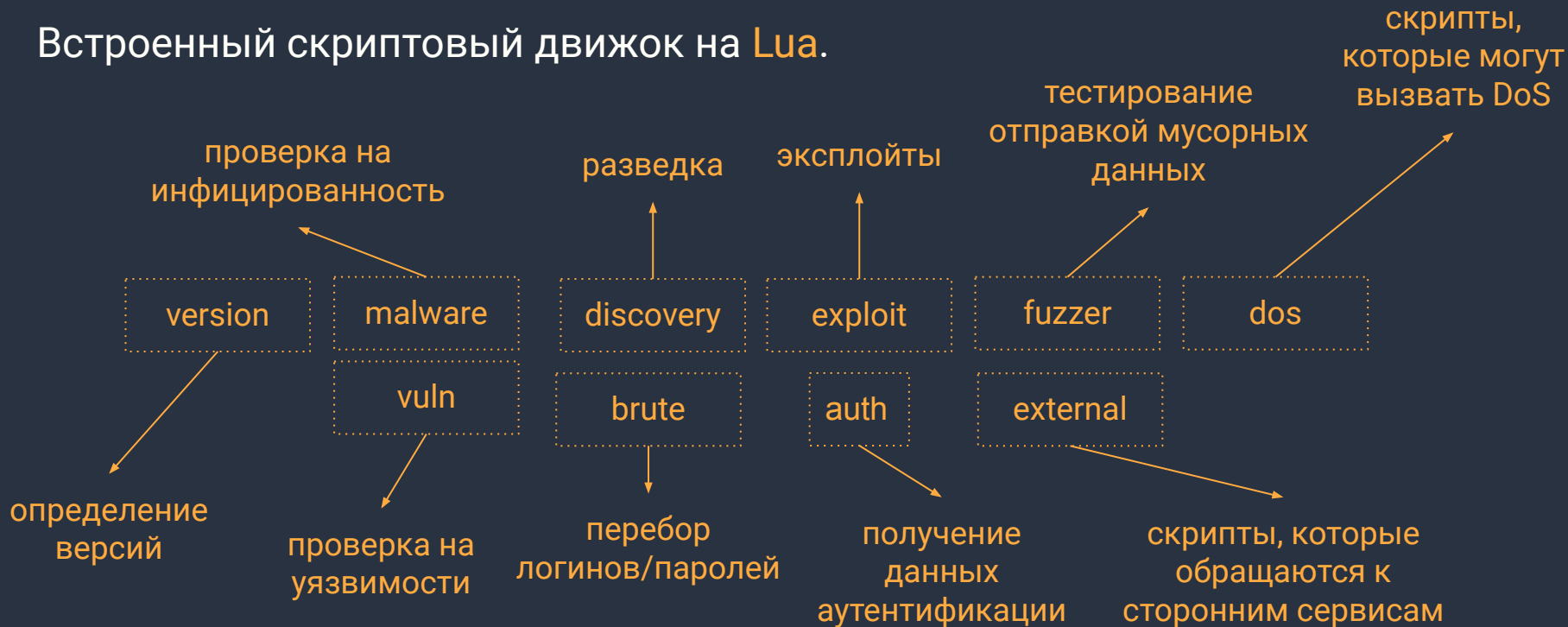


nmap.org



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

```
L$ 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:

Search:

Date	#	D	A	V	Title	Type	Platform	Author
2021-01-08	↓	✓			Apache Flink 1.11.0 - Unauthenticated Arbitrary File Read (Metasploit)	WebApps	Java	SunCSR Team
2020-11-24	↓	✗			Apache OpenMeetings 5.0.0 - 'hostname' Denial of Service	WebApps	Multiple	SunCSR
2020-11-17	↓	✗			Apache Struts 2.5.20 - Double OGNL evaluation	Remote	Multiple	West Shepherd
2020-11-13	↓	✓			Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit)	WebApps	Multiple	SunCSR

exploit-db.com

← → ↻ nvd.nist.gov/vuln/search/results?form_type=A... 🔍 ☆ ASP.NET

There are **248** matching records.
Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 > >>

Vuln ID	Summary	CVSS Severity
CVE-2020-9490	Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.	V3.1: 7.5 HIGH V2.0: 5.0 MEDIUM
Published: августа 07, 2020; 12:15:12 PM -0400		
CVE-2020-11993	Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.	V3.1: 7.5 HIGH V2.0: 4.3 MEDIUM
Published: августа 07, 2020; 12:15:11 PM -0400		

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>