

공격자 kali-linux

공격대상 Metasploitable && beebbox

## Nmap을 활용한 정보 수집

1. 네트워크 스캔을 해서 공격대상을 파악
2. nmap도구로 공격대상에 노출되어 있는 포트  
--> 많은 포트가 노출된다 --> 들어갈 수 있는 문이 많다. !

```
sudo nmap -p- 192.168.52.129
```

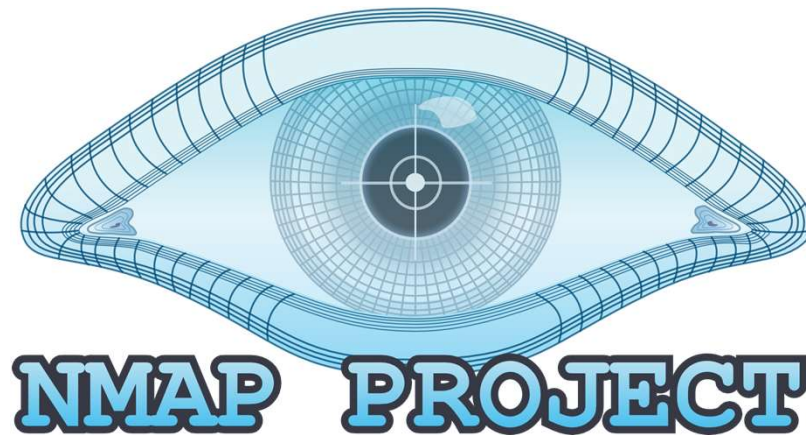
모든 포트를 다 검색하는 옵션

포트의 갯수 (1 ~ 65505)

# Nmap을 활용한 정보 수집

## Nmap

- Nmap은 Network Mapper의 약자
- 네트워크 검색 및 보안 감사를 위한 무료 오픈 소스(라이선스) 유틸리티
- 네트워크에서 사용할 수 있는 호스트, 해당 호스트가 제공하는 서비스(애플리케이션 이름 및 버전), 실행 중인 운영체제(및 OS 버전), 사용 중인 패킷 필터/방화벽 및 기타 수집 가지 특성 파악 가능
- 포트 스캔 도구 역할로 침투 테스트의 정보 수집 단계에서 가장 많이 활용
- 스크립트를 활용하면 NFS, SMB, RPC 등의 상세한 서비스 정보들을 수집할 수 있으며, 도메인 lookup, Whois 검색, 다른 네트워크 대역 서버의 백도어 설치 여부, 취약점 여부 등 많은 작업을 수행



```
sudo nmap -p- -sV 192.168.81.129
```

```
# 1번부터 80번 포트까지 스캔
```

```
sudo nmap -p1-80 -sV 192.168.81.129
```

# Nmap을 활용한 정보 수집

## Nmap 도움말

옵션	설명
-p <port ranges>	- 지정된 포트만 검색 - 예) -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
-p-	- 모든 포트 검색 (1~65535, 포트 0은 검색되지 않음)
--exclude-ports <port ranges>	- 지정된 포트를 제외하고 검색 - 예) --exclude-ports 22; --exclude-ports 80-100;
-sS	- TCP SYN 스캔 (기본 옵션)
-sT	- 기본 옵션으로 TCP Connect() 스캔
-sV	- 열린 포트를 조사하여 서비스/버전 정보 확인
-O	- 운영체제 탐지 활성화
-A	- 운영체제 탐지, 버전 탐지, 스크립트 스캐닝 및 traceroute 사용
-T<0-5>	- 타이밍 템플릿 설정으로 숫자가 높을수록 빠름
-oX <file>	- 주어진 파일 이름에 대해 XML 형태로 결과 출력
-d	- 스크립트 진행 상세 내역 모니터링 가능
-dd	- 더욱더 상세 내역 모니터링 가능
-oX	- XML 타입의 출력 스캔을 주어진 파일 이름으로 출력
--packet-trace	- 모든 네트워크 패킷의 상세 정보를 제공
--script-trace	- NSE(Nmap Scripting Engine) 스크립트에 대한 자세한 정보를 제공
-v	- 스캔하는 자세한 정보를 표시(더 자세한 정보는 -vv 사용)

# Nmap을 활용한 정보 수집

## 디버깅 옵션 활용

- -d 옵션을 사용하여 스크립트 진행 상세 내역 모니터링 가능

### -d 옵션

...(생략)...

NSE: Script scanning 192.168.180.137.

NSE: Starting runlevel 1 (of 1) scan.

NSE: Starting http-tomcat-brute against 192.168.180.137:8180.

Initiating NSE at 08:36

NSE: http-tomcat-brute against 192.168.180.137:8180 threw an error!

/usr/bin/./share/nmap/scripts/http-tomcat-brute.nse:112: variable 'brute' is not declared  
stack traceback:

[C]: in function 'error'

/usr/bin/./share/nmap/nselib/strict.lua:80: in function '\_\_index'

/usr/bin/./share/nmap/scripts/http-tomcat-brute.nse:112: in function

</usr/bin/./share/nmap/scripts/http-tomcat-brute.nse:108>

(...tail calls...)

Completed NSE at 08:36, 0.00s elapsed

...(생략)...

```
sudo nmap -p1-80 -sV -O 192.168.81.129
```

```
sudo nmap -p1-80 -A 192.168.81.129
```

# Nmap을 활용한 정보 수집

## ▶ 디버깅 옵션 활용

- -dd 옵션을 사용할 시에는 더욱더 상세 내역 모니터링 가능

### -dd 옵션

```
...(생략)...  
Fetchfile found C:\Program Files\Nmap\nse_main.lua  
Fetchfile found C:\Program Files\Nmap\nselib\stdnse.lua  
Fetchfile found C:\Program Files\Nmap\nselib\strict.lua  
Fetchfile found C:\Program Files\Nmap\scripts\script.db  
Fetchfile found C:\Program Files\Nmap\scripts\http-methods.nse  
NSE: Script http-methods.nse was selected by name.  
Fetchfile found C:\Program Files\Nmap\nselib\http.lua  
Fetchfile found C:\Program Files\Nmap\nselib\base64.lua  
Fetchfile found C:\Program Files\Nmap\nselib\comm.lua  
Fetchfile found C:\Program Files\Nmap\nselib\sasl.lua  
Fetchfile found C:\Program Files\Nmap\nselib\smbauth.lua  
Fetchfile found C:\Program Files\Nmap\nselib\url.lua  
Fetchfile found C:\Program Files\Nmap\nselib\shortport.lua  
NSE: Loaded 1 scripts for scanning.  
NSE: Loaded 'C:\Program Files\Nmap\scripts\http-methods.nse'.  
NSE: Script Pre-scanning.  
...(생략)...
```

# Nmap을 활용한 정보 수집

## 디버깅 옵션 활용

- 스크립트에서 자체 트레이스를 하기 위한 기능으로 --script-trace 활용

```
(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script-trace --script http-methods -p80 192.168.100.4
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-28 00:28 EDT
NSOCK INFO [0.8730s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.100.4:80]
NSE: TCP 192.168.100.3:48456 > 192.168.100.4:80 | CONNECT
NSE: TCP 192.168.100.3:48456 > 192.168.100.4:80 | 00000000: 16 03 00 00 69 01 00 00 65 03 03 55 1c a7 e4 72   i
e U r
00000010: 61 6e 64 6f 6d 31 72 61 6e 64 6f 6d 32 72 61 6e andom1random2ran
00000020: 64 6f 6d 33 72 61 6e 64 6f 6d 34 00 00 0c 00 2f dom3random4  /
00000030: 00 0a 00 13 00 39 00 04 00 ff 01 00 00 30 00 0d   9   0
00000040: 00 2c 00 2a 00 01 00 03 00 02 06 01 06 03 06 02 , *
00000050: 02 01 02 03 02 02 03 01 03 03 03 02 04 01 04 03
00000060: 04 02 01 01 01 03 01 02 05 01 05 03 05 02

NSOCK INFO [0.8730s] nsock_write(): Write request for 110 bytes to IOD #1 EID 19 [192.168.100.4:80]
NSOCK INFO [0.8730s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 19 [192.168.100.4:80]
NSE: TCP 192.168.100.3:48456 > 192.168.100.4:80 | SEND
NSOCK INFO [0.8740s] nsock_read(): Read request from IOD #1 [192.168.100.4:80] (timeout: 7000ms) EID 26
```

0~5 값이 존재하고, 값이 클수록 빠르다.

`sudo nmap -p1-80 -T3 192.168.81.129`

`sudo nmap -p1-80 -T2 192.168.81.129`

# Nmap을 활용한 정보 수집

## FTP 서비스 - Backdoor

- FTP는 File Transfer Protocol의 약자
- 컴퓨터 네트워크의 클라이언트와 서버 간에 컴퓨터 파일을 전송하는 데 사용되는 표준 네트워크 프로토콜
- FTP 기본 포트는 21번
- Metasploitable2는 널리 사용되는 FTP 서버인 vsftpd가 실행됨

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.100.5 -p21  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-28 07:59 EDT  
Nmap scan report for 192.168.100.5  
Host is up (0.00026s latency).  
  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.4  
Service Info: OS: Unix  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```



# Nmap NSE 활용



# Nmap NSE 활용

## NSE(Nmap Scripting Engine)이란?

- Lua 기반의 스크립트 언어를 이용하여 NFS, SMB, RPC 등의 상세한 정보 수집
- 다른 네트워크 대역의 백도어 설치 여부, 취약점 여부 판단 가능
- <https://nmap.org/nsedoc/>

**NSEDoc**

Index

NSE Documentation

**Categories**

auth

broadcast

brute

default

discovery

dos

exploit

external

fuzzer

intrusive

malware

safe

version

vuln

**Scripts (604)**

acarsd-info

address-info

afp-brute

**Scripts**

acarsd-info

address-info

afp-brute

afp-ls

afp-path-vuln

afp-serverinfo

afp-showmount

ajp-auth

ajp-brute

ajp-headers

Retrieves the authentication scheme and realm of an AJP service (Apache JServ Protocol) that requires authentication.

Performs brute force passwords auditing against the Apache JServ protocol. The Apache JServ Protocol is commonly used by web servers to communicate with back-end Java application server containers.

Performs a HEAD or GET request against either the root directory or any optional directory of an

kali@kali: /usr/share/nmap/scripts

File Actions Edit View Help

(kali@kali)-[~]  
\$ cd /usr/share/nmap/scripts

(kali@kali)-[/usr/share/nmap/scripts]  
\$ ls

acarsd-info.nse  
address-info.nse  
afp-brute.nse  
afp-ls.nse  
afp-path-vuln.nse  
afp-serverinfo.nse  
afp-showmount.nse  
ajp-auth.nse  
ajp-brute.nse  
ajp-headers.nse  
http-headers.nse  
http-hp-ilo-info.nse  
http-huawei-hg5xx-vuln.nse  
http-icloud-findmyiphone.nse  
http-icloud-sendmsg.nse  
http-iis-short-name-brute.nse  
http-iis-webdav-vuln.nse  
http-internal-ip-disclosure.nse  
http-joomla-brute.nse  
http-jsonp-detection.nse


# Nmap NSE 활용

## ▶▶ Nmap 개발

- 주요 모듈 및 스크립트 매월마다 업데이트 되는지 확인
- [NSE] 태그가 붙어 있는 것이 '스크립트'개발과 관련된 것이며, 정식으로 되어 있지 않지만 업무에 활용할 수 있는 도구 있음

[Current Quarter](#) [RSS Feed](#) [About List](#) [All Lists](#)

Unmoderated technical development forum for debating ideas, patches, and suggestions regarding proposed changes to [Nmap](#) and related projects. [Subscribe to nmap-dev here.](#)

List Archive Search 

### List Archives

	Jan-Mar	Apr-Jun	Jul-Sep	Oct-Dec
2022	<a href="#">10</a>	<a href="#">8</a>	—	—
2021	<a href="#">33</a>	<a href="#">14</a>	<a href="#">11</a>	<a href="#">15</a>
2020	<a href="#">12</a>	<a href="#">39</a>	<a href="#">29</a>	<a href="#">38</a>
2019	<a href="#">98</a>	<a href="#">44</a>	<a href="#">50</a>	<a href="#">16</a>
2018	<a href="#">55</a>	<a href="#">54</a>	<a href="#">49</a>	<a href="#">58</a>
2017	<a href="#">303</a>	<a href="#">199</a>	<a href="#">202</a>	<a href="#">68</a>

# Nmap NSE 활용

## ▶ 스크립트 카테고리 설명

- 카테고리, 라이브러리 정보 확인 가능
- <http://nmap.org/nsedoc/lib/nmap.html>

NMAP.ORG Site Search

Npcap.com Seclists.org Sectools.org Insecure.org

Download Reference Guide Book Docs Zenmap GUI In the Movies

NSEDoc	Scripts	Libraries	Categories
<b>Library nmap</b> Interface with Nmap internals. The nmap module is an interface port states and version detection Copyright © Same as Nmap--S <b>Functions</b> address family ()	acarsd-info address-info afp-brute afp-ls afp-path-vuln afp-serverinfo afp-showmount ajp-auth ajp-brute ajp-headers	afp ajp amqp anyconnect asn1 base32 base64 bin bitcoin bits	auth broadcast brute default discovery dos exploit external fuzzer intrusive

# 잘못사용하게 될 경우 서버가 터질 확률이 높은 명령어

## Nmap NSE 활용

### 카테고리 설명

카테고리	설명
auth	auth 카테고리는 대상 시스템의 인증 자격 범위를 다룬다. X11-access, ftp-anon, oracel-enum-users 등이 포함. 자격증명 부분을 무작위 대입 공격이 이루어지는 부분은 brute 카테고리에서 분류
broadcast	broadcast 카테고리에는 로컬 네트워크에서 broadcast를 이용하여, 호스트 정보들을 나열. Broadcast 의해서 호스트 정보들이 나열되지 않는 경우에, newtargets 스크립트 인수를 사용해서 호스트 발견 및 리스트에 나열을 하는 기능 포함
brute	brute 카테고리에는 대상 시스템의 인증 자격을 추측 대입 공격(Guessing)방식 등을 통해 무작위 대입 공격을 하는 기능이 포함. http-brute, oracle-brute, snmp-brute 등을 포함해서 다양한 프로토콜 및 서비스를 대상으로 이루어짐.
default	default 카테고리는 기본적으로 설정되어 있는 기능들이 포함되어 있다. -script=default 를 통해서도 사용될 수 있으며, 기본적인 설정만을 가지고 스크립트를 적용할 때 활용
discovery	discovery 카테고리는 레지스터리 정보, SNMP 정보, 디렉터리 정보 등 네트워크와 관련된 정보 추가 획득 사용
dos	dos 카테고리는 서비스 거부 공격(denial of service)을 수행할 시에 이용 (테스트 서버에서만 수행 바람)
exploit	exploit 카테고리는 특정 취약점을 이용하여 공격코드를 실행할 시 이용
external	external 카테고리는 외부에 존재하는 서비스를 이용해서 결과 값을 가져옴. 예로 whois를 통해 아이피 정보만을 이용해 정보를 획득하는 방식 이 포함
fuzzer	fuzzer 카테고리는 대상 시스템을 대상으로 네트워크, 서버에 임의의 값을 삽입하여 크래시가 발생하는지 판단하여 버그를 진단할 시 이용
intrusive	intrusive 카테고리는 대상 시스템에 심각한 영향을 줄 수 있기 때문에 safe 카테고리로 분류하지 않음
malware	malware 카테고리는 대상 시스템이 악성 코드나 백door 등이 설치 되어 있는지 여부를 간단히 검사 가능. 대부분 포트 정보 및 응답 값을 통해서 판단
safe	safe 카테고리는 시스템에 영향을 최소화 하면서 획득할 수 있는 스크립트 모음. intrusive 카테고리에 포함되지 않은 스크립트들이 포함.
version	version 카테고리는 대상 시스템에 포함되어 있는 서비스들의 버전 정보를 획득하는 데 이용.
vuln	vuln 카테고리는 알려진 취약점에 대해서 진단을 수행하며, 만약 존재하면 간단하게 보고서를 작성

# Nmap NSE 활용

## 카테고리 설명

카테고리	설명
auth	auth 카테고리는 대상 시스템의 인증 자격 범위를 다룬다. X11-access, ftp-anon, oracel-enum-users 등이 포함. 자격증명 부분을 무작위 대입 공격이 이루어지는 부분은 brute 카테고리에서 분류
broadcast	broadcast 카테고리에는 로컬 네트워크에서 broadcast를 이용하여, 호스트 정보들을 나열. Broadcast 의해서 호스트 정보들이 나열되지 않는 경우에, newtargets 스크립트 인수를 사용해서 호스트 발견 및 리스트에 나열을 하는 기능 포함
brute	brute 카테고리에는 대상 시스템의 인증 자격을 추측 대입 공격(Guessing)방식 등을 통해 무작위 대입 공격을 하는 기능이 포함. http-brute, oracle-brute, snmp-brute 등을 포함해서 다양한 프로토콜 및 서비스를 대상으로 이루어짐.
default	default 카테고리는 기본적으로 설정되어 있는 기능들이 포함되어 있다. -script=default 를 통해서도 사용될 수 있으며, 기본적인 설정만을 가지고 스크립트를 적용할 때 활용
discovery	discovery 카테고리는 레지스터리 정보, SNMP 정보, 디렉터리 정보 등 네트워크와 관련된 정보 추가 획득 사용
dos	dos 카테고리는 서비스 거부 공격(denial of service)을 수행할 시에 이용 (테스트 서버에서만 수행 바람)
exploit	exploit 카테고리는 특정 취약점을 이용하여 공격코드를 실행할 시 이용
external	external 카테고리는 외부에 존재하는 서비스를 이용해서 결과 값을 가져옴. 예로 whois를 통해 아이피 정보만을 이용해 정보를 획득하는 방식 이 포함
fuzzer	fuzzer 카테고리는 대상 시스템을 대상으로 네트워크, 서버에 임의의 값을 삽입하여 크래시가 발생하는지 판단하여 버그를 진단할 시 이용
intrusive	intrusive 카테고리는 대상 시스템에 심각한 영향을 줄 수 있기 때문에 safe 카테고리로 분류하지 않음
malware	malware 카테고리는 대상 시스템이 악성 코드나 백도어 등이 설치 되어 있는지 여부를 간단히 검사 가능. 대부분 포트 정보 및 응답 값을 통해서 판단
safe	safe 카테고리는 시스템에 영향을 최소화 하면서 획득할 수 있는 스크립트 모음. intrusive 카테고리에 포함되지 않은 스크립트들이 포함.
version	version 카테고리는 대상 시스템에 포함되어 있는 서비스들의 버전 정보를 획득하는 데 이용.
vuln	vuln 카테고리는 알려진 취약점에 대해서 진단을 수행하며, 만약 존재하면 간단하게 보고서를 작성



# Nmap NSE 활용

## 스크립트 주요 옵션

```
—(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script=default 192.168.100.4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-28 00:35 EDT
Nmap scan report for 192.168.100.4
Host is up (0.0095s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r-- 1 root    www-data  543803 Nov  2 2014 Iron_Man.pdf
| -rw-rw-r-- 1 root    www-data  462949 Nov  2 2014 Terminator_Salvation.pdf
| -rw-rw-r-- 1 root    www-data  544600 Nov  2 2014 The_Amazing_Spider-Man.pdf
| -rw-rw-r-- 1 root    www-data  526187 Nov  2 2014 The_Cabin_in_the_Woods.pdf
| -rw-rw-r-- 1 root    www-data  756522 Nov  2 2014 The_Dark_Knight_Rises.pdf
| -rw-rw-r-- 1 root    www-data  618117 Nov  2 2014 The_Incredible_Hulk.pdf
|_ -rw-rw-r-- 1 root    www-data  5010042 Nov  2 2014 bWAPP_intro.pdf
22/tcp    open  ssh
| ssh-hostkey:
| 1024 45:a4:66:ec:3a:ba:97:f8:3e:1a:ba:1c:24:68:22:e8 (DSA)
|_ 2048 63:e7:c5:d1:8d:8a:94:02:36:6a:d7:d2:75:e9:8b:ce (RSA)
25/tcp    open  smtp
|_ smtp-commands: bee-box, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ ssl-date: 2021-03-28T04:37:04+00:00; +4s from scanner time.
| sslv2:
|  SSLv2 supported
80/tcp    open  http
| http-methods:
|_  Potentially risky methods: TRACE
|_ http-title: Site doesn't have a title (text/html).
```

# Nmap NSE 활용

## NSE 도움말

옵션	설명
-sC	<ul style="list-style-type: none"> <li>- default 스크립트 세트를 사용하여 스크립트 스캔을 수행</li> <li>- --script=default와 동일</li> <li>- 예) <b>nmap -sC</b></li> </ul>
--script <filename> <category> <directory> <expression>[,...]	<ul style="list-style-type: none"> <li>- 파일 이름, 스크립트 카테고리 및 디렉터리 목록을 사용하여 스크립트 스캔 실행</li> <li>- Boolean 표현식으로 사용 가능</li> <li>- 스크립트를 이름으로 참조할 때 '*' 와일드카드 사용 가능</li> <li>- 예1) <b>nmap --script "http-*</b></li> <li>- 설명1) http-auth 및 http-open-proxy와 같이 이름이 http-로 시작하는 모든 스크립트 로드</li> <li>- 예2) <b>nmap --script "default or safe"</b></li> <li>- 설명2) default 카테고리나 safe 카테고리 또는 둘 다 존재하는 모든 스크립트 로드</li> <li>- 예3) <b>nmap --script "default and safe"</b></li> <li>- 설명3) default 및 safe 카테고리 모두에 속한 스크립트를 로드</li> </ul>
--script-trace	<ul style="list-style-type: none"> <li>- NSE(Nmap Scripting Engine) 스크립트에 대한 자세한 정보를 제공</li> <li>- 표시되는 정보에는 통신 프로토콜, 소스, 대상 및 전송된 데이터가 포함됨</li> </ul>
--script-help <filename> <category> <directory> <expression> all[,...]	<ul style="list-style-type: none"> <li>- 스크립트에 대한 도움말 출력</li> <li>- 주어진 스크립트에 대해 Nmap은 스크립트 이름, 카테고리 및 설명을 출력</li> <li>- 예) <b>nmap --script-help ftp-anon</b></li> <li>- 예) <b>nmap --script-help default</b></li> </ul>
--script-updatedb	<ul style="list-style-type: none"> <li>- 사용 가능한 기본 스크립트와 카테고리를 결정하기 위해 Nmap이 사용하는 scripts/script.db에 있는 스크립트 데이터베이스를 업데이트함</li> <li>- 기본 스크립트 디렉터리에서 NSE 스크립트를 추가 또는 제거했거나 스크립트 카테고리를 변경한 경우에만 데이터베이스 업데이트 필요</li> </ul>

# Nmap NSE 활용

## 스크립트 위치

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ cat script.db | more
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "afp-path-vuln.nse", categories = { "exploit", "intrusive", "vuln", } }
Entry { filename = "afp-serverinfo.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "afp-showmount.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ajp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "ajp-headers.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-methods.nse", categories = { "default", "safe", } }
Entry { filename = "ajp-request.nse", categories = { "discovery", "safe", } }
Entry { filename = "allseeingeeye-info.nse", categories = { "discovery", "safe", "version", } }
Entry { filename = "amqp-info.nse", categories = { "default", "discovery", "safe", "version", } }
Entry { filename = "asn-query.nse", categories = { "discovery", "external", "safe", } }
Entry { filename = "auth-owners.nse", categories = { "default", "safe", } }
Entry { filename = "auth-spoof.nse", categories = { "malware", "safe", } }
Entry { filename = "backorifice-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "backorifice-info.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "bacnet-info.nse", categories = { "discovery", "version", } }
Entry { filename = "banner.nse", categories = { "discovery", "safe", } }
Entry { filename = "bitcoin-getaddr.nse", categories = { "discovery", "safe", } }
Entry { filename = "bitcoin-info.nse", categories = { "discovery", "safe", } }
```



# Nmap NSE 활용

## 업무 활용 스크립트

- 취약점 분석 데이터베이스 활용 - **vulscan.nse**
- CVE([Common Vulnerabilities and Exposures](#))의 데이터베이스를 비롯하여 다양한 취약점 데이터베이스를 비교한 결과를 스캔한 정보와 결합을 하여 출력

데이터베이스 파일	사이트 정보
scipvuldb.csv	<a href="https://vuldb.com">https://vuldb.com</a>
cve.csv	<a href="http://cve.mitre.org">http://cve.mitre.org</a>
securityfocus.csv	<a href="http://www.securityfocus.com/bid/">http://www.securityfocus.com/bid/</a>
xforce.csv	<a href="https://exchange.xforce.ibmcloud.com/">https://exchange.xforce.ibmcloud.com/</a>
exploitdb.csv	<a href="https://www.exploit-db.com">https://www.exploit-db.com</a>
openvas.csv	<a href="http://www.openvas.org">http://www.openvas.org</a>
securitytracker.csv	<a href="https://www.securitytracker.com">https://www.securitytracker.com</a> (end-of-life)
osvdb.csv	<a href="http://www.osvdb.org">http://www.osvdb.org</a> (end-of-life)

# Nmap NSE 활용

## 업무 활용 스크립트

### ● 취약점 분석 데이터베이스 활용 - vulscan.nse

NSE – vulscan.nse를 이용하여 취약점 분석

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ sudo nmap -sV --script=vulscan/vulscan.nse 192.168.100.62 -p21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 21:15 EST
Nmap scan report for 192.168.100.62
Host is up (0.00056s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| vulscan: VulDB - https://vuldb.com:
| [146452] vsftpd 2.3.4 Service Port 6200 privilege escalation
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2011-0762] The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated
| (denial of service via resource exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [82285] Vsftpd CVE-2004-0042 Remote Security Vulnerability
| [72451] vsftpd CVE-2015-1419 Security Bypass Vulnerability
| [51013] vsftpd '__tzfile_read()' Function Heap Based Buffer Overflow Vulnerability
| [48539] vsftpd Compromised Source Packages Backdoor Vulnerability
| [46617] vsftpd FTP Server 'ls.c' Remote Denial of Service Vulnerability
| [41443] Vsftpd Webmin Module Multiple Unspecified Vulnerabilities
| [30364] vsftpd FTP Server Pluggable Authentication Module (PAM) Remote Denial of Service Vulnerability
| [29322] vsftpd FTP Server 'deny_file' Option Remote Denial of Service Vulnerability
| [10394] Vsftpd Listener Denial of Service Vulnerability
| [7253] Red Hat Linux 9 vsftpd Compiling Error Weakness
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [68366] vsftpd package backdoor
```



# Nmap NSE 스크립트 개발

# Nmap NSE 스크립트 개발

## NSE 포맷 설명

옵 션	내 용
Description Filed	스크립트가 어떤 것을 테스트하는지와 사용자가 알아야 할 중요한 사항에 대해 설명
Categories Filed	스크립트가 속하는 하나 이상의 범주를 정의 스크립트의 용도에 따라 2가지 이상 항목에 포함이 되어 있다면 카테고리 이름을 모두 포함
Author Filed	스크립트 작성자의 이름이 포함되며 연락처 정보(예: 홈 페이지 URL)도 포함 가능
License Filed	엔맵 커뮤니티 프로젝트에서 라이브러리를 제공하고 있으며, 사용자들이 각자의 스크립트를 작성하더라도 배포할 시에 라이선스에 대한 표시
Dependencies Filed	스크립트를 실행하는데 다른 스크립트들이 필요할 시에 표시 이 스크립트보다 먼저 실행해야 하는 스크립트의 이름을 포함하는 배열
Rules	포트나 호스트, 서비스 등 여러 규칙이 포함, 해당 규칙일 경우에만 Action의 코드 실행 prerule(), hostrule(host), portrule(host, port), postrule()
Action	Rules에서 정의한 규칙을 만족할 때, 실제로 실행될 수 있는 모든 코드들이 포함 portrule이 일치가 되었을 때 메인함수라고 할 수 있는 action=function 이 실행

# Nmap NSE 스크립트 개발

## 첫 걸음 - HelloWorld

```
-- The Head Section --
---- http 모듈을 가져와서 http 변수에 할당 ----
local http = require "http"

description = [[
  Outputs "Hello world!" if HTTP port (80) is open.
]]

categories = {"default"}

-- The Rule Section --
---- portrule 함수에서는 스캔 대상과 호스트와 포트에 대한 조건 지정 ----
---- TCP 프로토콜을 사용하며, 포트 번호가 80이고, 해당 포트가 열려 있을 때 실행 ----
portrule = function(host, port)
  return port.protocol == "tcp" and port.number == 80 and port.state == "open"
end

-- The Action Section --
---- action 함수에서는 스캔 대상 호스트와 포트에 대한 액션 지정 ----
---- http 모듈을 사용하여 스캔 대상 호스트에 HTTP GET 요청 전송 ----
---- 응답 상태 코드가 200인 경우 "Hello world!" 문자열 반환 ----
action = function(host, port)
  local result = http.get(host, port, "/")
  if result.status == 200 then
    return "Hello world!"
  end
end
```

응답코드

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV --script=hello 192.168.100.5 -p80
Starting Nmap 7.91 ( https://nmap.org )
Nmap scan report for 192.168.100.5
Host is up (0.00033s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_hello:  Hello world!
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
MAC Address: 00:0C:29:3D:DE:90 (VMware)
```

# lua 언어

## Nmap NSE 스크립트 개발

### 서비스 응답/요청 테스트 - Twiki 검증

-- TWiki는 Perl로 작성된 공개 소프트웨어이며, 다양한 기능을 갖춘 웹 기반 협업 플랫폼 --

```
local shortport = require "shortport"
local http = require "http"
```

```
description = [[ Service Test Page ]]      [[string]]
categories = {"safe"}
```

-- The Rule Section --

---- HTTP 프로토콜을 사용하는 포트 기본 값(80, 81, 3080, 8080, 8180, 8443)에 스크립트 적용 정의 ----

```
portrule = shortport.http
```

-- The Action Section --

---- 지정된 URI로 HTTP GET 요청을 전송하고, ----

---- 응답 상태 코드가 200이면 응답 바디를 반환 ----

```
action = function(host, port)
  local uri = "/twiki/TWikiDocumentation.html"
  local response = http.get(host, port, uri)
  if(response.status == 200) then
    return response.body
  end
end
```

# Nmap NSE 스크립트 개발

## ▶ 서비스 응답/요청 테스트 - Twiki 검증

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV --script=twiki 192.168.100.5 -p80,8180 | head -n 50
Starting Nmap 7.91 ( https://nmap.org )
Nmap scan report for 192.168.100.5
Host is up (0.00032s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|twiki: <html><head>
|<title>TWikiDocumentation</title>
|</head><body bgcolor="#ffffff">
|<h1><a name="_TWiki_Reference_Manual_01_Feb_2"> TWiki Reference Manual (01 Feb 2003) </a></h1>
|<p />
|<script language="JavaScript1.2" type="text/javascript">
|<!--
|function dblclick() { window.scrollTo(0,0) }
|if (document.layers) { document.captureEvents(ONDBLCLICK); }
|document.ondblclick=dblclick;
|→
|</script>
|<p />
|This page contains all documentation topics as one long, complete reference sheet.<br />
|<strong><em>Doubleclick anywhere</em></strong> to return to the top of the page.
|<p />
```



# Nmap NSE 스크립트 개발

## ▶ 톰캣 버전 정보 확인 스크립트 개발

```
local shortport = require "shortport"
local http = require "http"
local stdnse = require "stdnse"
```

```
description = [[
Version Check
]]
```

```
categories = {"safe","version"}
```

```
-- The Rule Section --
portrule = shortport.http
```

```
-- The Action Section --
action = function(host, port)
```

```
    local uri = "/"
    local response = http.get(host, port, uri)
```

```
    if ( response.status == 200 ) then
        local title = string.match(response.body, "<[Tt][Ii][Tt][Ll][Ee][^>]*>([<]*)/[Tt][Ii][Tt][Ll][Ee]>")
        return title
    end
```

```
end
```

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ sudo nmap -sV --script=tomcat_version 192.168.100.5 -p8180
Starting Nmap 7.91 ( https://nmap.org )
Nmap scan report for 192.168.100.5
Host is up (0.00020s latency).

PORT      STATE SERVICE VERSION
8180/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_tomcat_version: Apache Tomcat/5.5
MAC Address: 00:0C:29:3D:DE:90 (VMware)
```