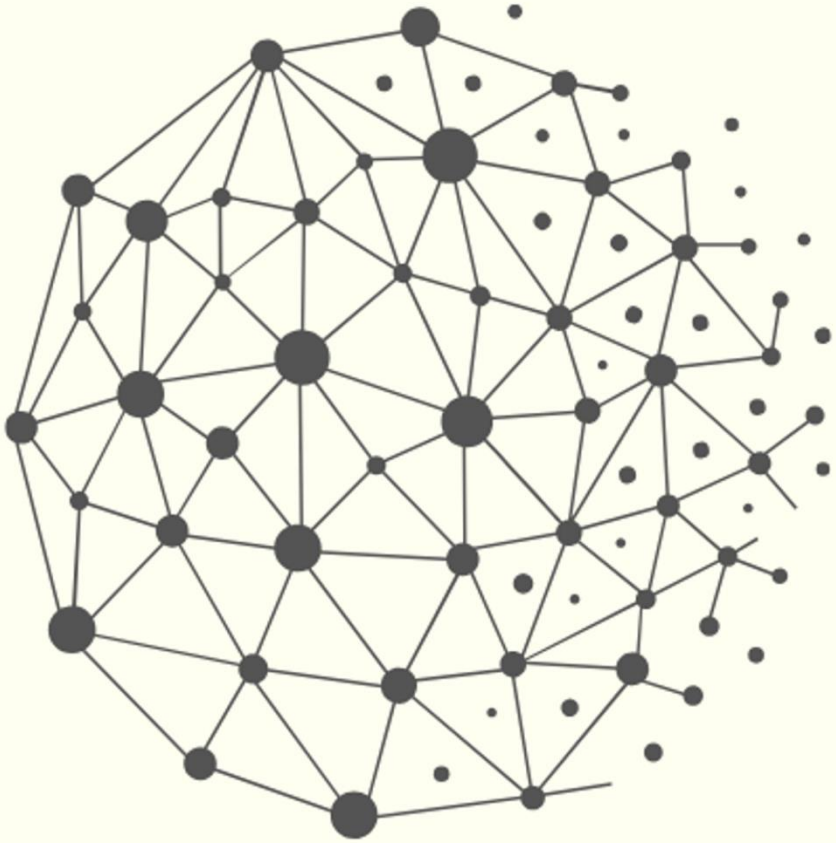


Blue Team 보고서

Supernova

TEAM-DEVSECOPS

목차

모의해킹용 쉘 스크립트 3

◈ 모의해킹용 쉘 스크립트 3

◈ 스크립트 실행 방법 4

◈ 로그 파일 5

◈ 요구 사항 5

◈ 스크립트 실행 예시 결과 6

◈ 블루팀 멤버

소속	성명	담당 업무
Team DevSecOps	장진영	● 모의해킹용 쉘 스크립트 작성
	안정훈	● nmap, dirb, gobuster, nikto 도구 활용 쉘 스크립트 작성

모의해킹용 쉘 스크립트

Shell script for scanning on kali linux

◈ 모의해킹용 쉘 스크립트

Kali Linux 를 이용한 모의해킹을 위하여 Kali Linux 에 있는 다양한 스캐닝도구에 대한 자동화 쉘 스크립트를 작성했습니다.

<table>
<tr><th colspan="4">칼리 리눅스 쉘 스크립트</th></tr>
<tr><td>수 행 인 원</td><td colspan="2">장진영, 안정훈</td><td>작 성 자 : 장진영</td></tr>
<tr><td>제 목</td><td colspan="3">Kali Linux 모의해킹용 도구 자동화 Shell Script</td></tr>
<tr><td>내 용</td><td colspan="3">Kali Linux 의 모의 해킹 도구 중 스캐닝 도구를 활용한 자동화 쉘 스크립트를 작성했습니다. 사용한 도구는 포트 스캐닝을 위한 nmap, 취약점 분석을 위한 nikto, 디렉토리 및 파일 스캐닝을 위한 dirb 와 gobuster 등 총 4 가지입니다. 이 스크립트는 각 도구를 실행하고, 결과를 출력하며 로그를 남기는 기능을 제공합니다.</td></tr>
<tr><td rowspan="6">결 과 물</td><td>No</td><td>스크립트</td><td>설명</td></tr>
<tr><td>1</td><td>attack.sh</td><td>1) 메인 실행 스크립트
2) 사용 가능한 스캐닝 도구들을 메뉴로 제공
3) 사용자가 선택한 스크립트를 실행
4) 로그 디렉토리 자동 생성 및 관리
5) 전체 실행 세션을 logs/attack/ 디렉토리에 저장</td></tr>
<tr><td>2</td><td>nmap.sh</td><td>1) 포트 스캐닝 도구
2) 대상 IP 의 열린 포트, 서비스, 버전 정보를 스캔
3) 결과를 테이블 형식으로 표시
4) 상태에 따른 컬러 출력 지원 (열린 포트: 초록색, 닫힌 포트: 빨간색)
5) 스캔 결과는 logs/nmap/ 디렉토리에 저장</td></tr>
<tr><td>3</td><td>nikto.sh</td><td>1) 웹 서버 취약점 스캐닝 도구
2) 웹 서버의 알려진 취약점을 검사
3) 위험도에 따른 결과 분류 (Low, Medium, High)
4) 컬러 출력으로 위험도 구분
5) 스캔 결과는 logs/nikto/ 디렉토리에 저장</td></tr>
<tr><td>4</td><td>dirb.sh</td><td>1) 디렉토리 브루트포스 스캐닝 도구
2) 웹 서버의 숨겨진 디렉토리와 파일을 검색
3) 기본 워드리스트: common.txt
4) 발견된 항목을 디렉토리와 파일로 구분하여 표시
5) HTTP 상태 코드에 따른 컬러 출력 지원
6) 스캔 결과는 logs/dirb/ 디렉토리에 저장</td></tr>
<tr><td>5</td><td>gobuster.sh</td><td>1) 디렉토리 및 파일 브루트포스 스캐닝 도구
2) 웹 서버의 숨겨진 디렉토리와 파일을 검색
3) 기본 워드리스트: common.txt</td></tr>
</table>

			4) 기본 확장자: html, php, txt 5) 발견된 항목을 디렉토리와 파일로 구분하여 표시 6) 파일 타입별 구분 (HTML, PHP, TXT 등) 7) 기본 워드리스트 또는 사용자 정의 워드리스트 선택 가능 8) 기본 탐색 파일 확장자 또는 사용자 정의 확장자 선택 가능 9) 스캔 결과는 logs/gobuster/ 디렉토리에 저장

◈ 스크립트 실행 방법

스크립트 실행 방법			
수 행 인 원	장진영, 안정훈	작 성 자	장진영
제 목	작성 Shell Scripts 실행 방법		

No	내용	설명
1	스크립트 실행	`./attack.sh` 명령어를 입력하여 메인 스크립트 실행
2	스캐닝 도구 선택	1. Nmap Port Scanner : Nmap 도구 사용 2. Nikto Web Scanner: Nikto 도구 사용 3. Dirb Directory Scanner: Dirb 도구 사용 4. Gobuster Directory Scanner: Gobuster 도구 사용 5. Exit: 스캐닝
3	필요 정보 입력	Nmap: 대상 IP 주소 (ex: 192.168.1.1) Nikto/Dirb/Gobuster: 1. 대상 URL (ex: http://192.168.1.1 또는 http://domain.com) 2. 워드리스트 선택 (기본 또는 사용자 정의 3. Gobuster 의 경우 파일 확장자 선택 가능 (ex: html, php, txt)
4	입력 정보 확인	입력한 정보가 맞는지 확인 (y/n)하고 틀린 경우 재입력 가능
5	스캔 결과 확인	실시간을 화면에 출력 및 자동으로 logs 디렉토리에 저장
6	추가 스캔	스캔 완료 후 추가 스캔 여부 선택 가능 이전 스캔 결과가 화면에 유지된 상태로 계속 진행

◈ 로그 파일

이 모의해킹용 쉘 스크립트의 모든 과정은 자동으로 logs 디렉터리 아래에 로그 파일을 남겨 이후에도 이전에 사용한 도구들의 결과에 대한 로그를 확인할 수 있습니다. 모든 로그파일명에는 타임스탬프를 포함하며 각 도구에 따라 저장되는 최종 디렉터리는 아래와 같습니다.

```
logs/
    ├─── nmap/ : 포트 스캔 결과
    ├─── nikto/ : 취약점 스캔 결과
    ├─── dirb/ : 디렉토리/파일 스캔 결과
    ├─── gobuster/ : 디렉토리/파일 스캔 결과
    └─── attack/ : 전체 실행 세션 로그
```

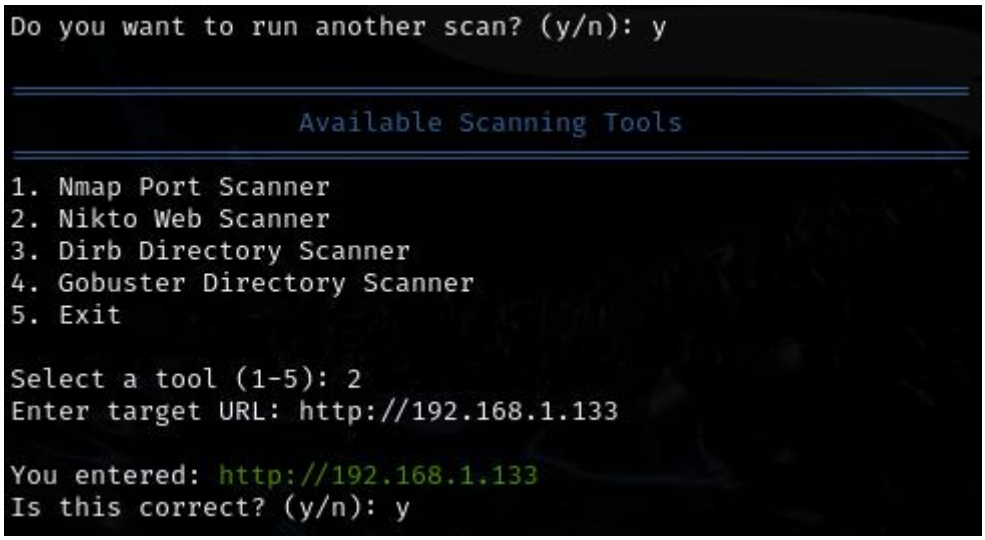
◈ 요구 사항

- Kali Linux 운영체제
- nikto 설치
- nmap 설치
- dirb 설치
- gobuster 설치

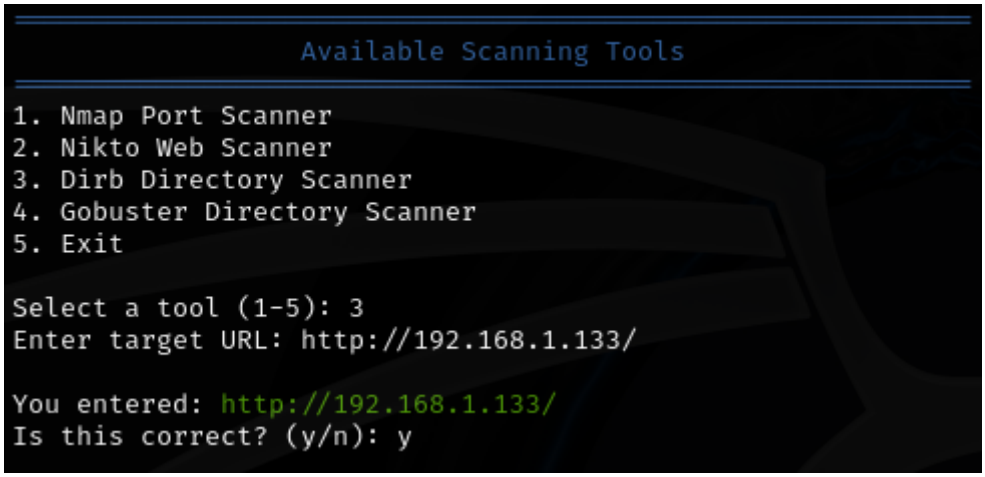
◈ 스크립트 실행 예시 결과

attack.sh 실행 결과

1) Nmap Port Scanner 선택 시



2) 추가 스캔 선택 후 Nikto Web Scanner 선택 시



3) Dirb Directory Scanner 선택 시

```
                Available Scanning Tools

1. Nmap Port Scanner
2. Nikto Web Scanner
3. Dirb Directory Scanner
4. Gobuster Directory Scanner
5. Exit

Select a tool (1-5): 4
Enter target URL: http://192.168.1.133

You entered: http://192.168.1.133
Is this correct? (y/n): y
```

4) Gobuster Directory Scanner 선택 시

```
                Available Scanning Tools

1. Nmap Port Scanner
2. Nikto Web Scanner
3. Dirb Directory Scanner
4. Gobuster Directory Scanner
5. Exit

Select a tool (1-5): 5
Exiting...

[+] Attack session ended at 2025-01-22 21:38:49
[+] Attack log saved to: logs/attack/attacklog20250122_213848.log
```

5) Exit 선택 시

nmap.sh 실행 결과

```
                NMAP SCANNING RESULT

[+] Scan completed for 192.168.1.133 using Nmap

[+] Discovered Ports:
+-----------+-----------+-----------------+-----------------------------------------+
| PORT      | STATE     | SERVICE         | VERSION                                 |
+-----------+-----------+-----------------+-----------------------------------------+
| 22/tcp    | open      | ssh             | OpenSSH 8.7 (protocol 2.0)              |
| 80/tcp    | open      | http            | Apache httpd 2.4.57 ((Rocky Linux))     |
| 443/tcp   | closed    | https           |                                         |
| 8080/tcp  | closed    | http-proxy      |                                         |
| 9090/tcp  | closed    | zeus-admin      |                                         |
| 9091/tcp  | closed    | xmltec-xmlmail  |                                         |
| 30000/tcp | closed    | ndmps           |                                         |
+-----------+-----------+-----------------+-----------------------------------------+

[+] NMAP scanning log saved to: ../logs/nmap/nmapscan20250122_211810.log
```

nikto.sh 실행 결과

```
═══════════════════════════════════════════════════════════
                    NIKTO SCANNING RESULT
═══════════════════════════════════════════════════════════

[+] Scan completed for http://192.168.1.133 using Nikto

[+] Scan Results by Risk Level:

Risk Level Indicators:
■ Information
■ Low Risk
■ Medium Risk
■ High Risk

[*] Information Level Findings
+--------------------------+---------------------------------------------------------------------------------
| CATEGORY                 | FINDING
+--------------------------+---------------------------------------------------------------------------------
| DIRECTORY ACCESS         | Directory listing enabled in /db/
| OTHER                    | /css/: This might be interesting.
| DIRECTORY ACCESS         | Directory listing enabled in /css/
| CONFIGURATION            | Sensitive information in robots.txt
| SERVER INFO              | Server technology exposed: PHP/8.0.30.
| SERVER INFO              | Web Server: Apache/2.4.57 (Rocky Linux)
| SCAN INFO                | Start Time:         2025-01-22 21:26:01 (GMT-5)
| SCAN INFO                | Port: 80
| SCAN INFO                | Target Hostname:    192.168.1.133
| SCAN INFO                | Target IP: 192.168.1.133
| OTHER                    | 1 host(s) tested
| OTHER                    | 8910 requests: 0 error(s) and 20 item(s) reported on remote host
| SCAN INFO                | End Time:           2025-01-22 21:26:23 (GMT-5) (22 seconds)
| OTHER                    | /php/: This might be interesting.
| DIRECTORY ACCESS         | Directory listing enabled in /icons/
| OTHER                    | /db/: This might be interesting.
| DIRECTORY ACCESS         | Directory listing enabled in /php/
| SENSITIVE FILES          | Composer configuration exposed in /composer.lock
| SECURITY HEADERS         | Cookies missing HttpOnly flag
| SENSITIVE FILES          | /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-ac
| SENSITIVE FILES          | Composer configuration exposed in /composer.json
+--------------------------+---------------------------------------------------------------------------------

[+] Low Risk Findings
+--------------------------+---------------------------------------------------------------------------------
| CATEGORY                 | FINDING
+--------------------------+---------------------------------------------------------------------------------
| SECURITY HEADERS         | Missing MIME Protection
| SECURITY HEADERS         | Missing Clickjacking Protection
+--------------------------+---------------------------------------------------------------------------------

[!] Medium Risk Findings
+--------------------------+---------------------------------------------------------------------------------
| CATEGORY                 | FINDING
+--------------------------+---------------------------------------------------------------------------------
| HTTP METHODS             | HTTP TRACE method enabled
| HTTP METHODS             | HTTP TRACE method enabled
+--------------------------+---------------------------------------------------------------------------------

[!!] High Risk Findings
+--------------------------+---------------------------------------------------------------------------------
| CATEGORY                 | FINDING
+--------------------------+---------------------------------------------------------------------------------
| SENSITIVE FILES          | Git repository files exposed in /.git/config
| SENSITIVE FILES          | Git repository files exposed in /.git/HEAD
| SENSITIVE FILES          | Git repository files exposed in /.git/index
+--------------------------+---------------------------------------------------------------------------------
```

dirb.sh 실행 결과

```
═══════════════════════════════════════════════
                DIRB SCANNING RESULT
═══════════════════════════════════════════════

Do you want to use a custom wordlist? (default: /usr/share/dirb/wordlists/common.txt)
Enter y/n: n

Using wordlist: /usr/share/dirb/wordlists/common.txt

[+] Scan completed for http://192.168.1.133/ using Dirb

[+] Discovered Directories:
+---------+-----------------------------------+---------+---------+
| TYPE    | PATH                              | STATE   | SIZE    |
+---------+-----------------------------------+---------+---------+
| DIR     | http://192.168.1.133/assets/      | 301     | N/A     |
| DIR     | http://192.168.1.133/components/  | 301     | N/A     |
| DIR     | http://192.168.1.133/css/         | 301     | N/A     |
| DIR     | http://192.168.1.133/db/          | 301     | N/A     |
| DIR     | http://192.168.1.133/icon/        | 301     | N/A     |
| DIR     | http://192.168.1.133/js/          | 301     | N/A     |
| DIR     | http://192.168.1.133/path/        | 301     | N/A     |
| DIR     | http://192.168.1.133/php/         | 301     | N/A     |
| DIR     | http://192.168.1.133/uploads/     | 301     | N/A     |
| DIR     | http://192.168.1.133/vendor/      | 301     | N/A     |
| DIR     | http://192.168.1.133/cgi-bin/     | 403     | 199     |
+---------+-----------------------------------+---------+---------+

[+] Discovered Files:
+---------+-----------------------------------+---------+---------+
| TYPE    | PATH                              | STATE   | SIZE    |
+---------+-----------------------------------+---------+---------+
| FILE    | http://192.168.1.133/.git/HEAD    | 200     | 23      |
| HTML    | http://192.168.1.133/index.html   | 200     | 20925   |
| TXT     | http://192.168.1.133/robots.txt   | 200     | 58      |
+---------+-----------------------------------+---------+---------+

[+] DIRB scanning log saved to: ../logs/dirb/dirbscan20250122_213026.log
```

gobuster.sh 실행 결과

```
═══════════════════════════════════════════════
                GOBUSTER SCANNING RESULT
═══════════════════════════════════════════════

Do you want to use a custom wordlist? (default: /usr/share/dirb/wordlists/common.txt)
Enter y/n: n

Do you want to use custom extensions? (default: html,php,txt)
Enter y/n: y

Enter extensions (comma-separated, no spaces): html,txt,json

Using wordlist: /usr/share/dirb/wordlists/common.txt
Using extensions: html,txt,json

[+] Scan completed for http://192.168.1.133 using Gobuster

[+] Discovered Directories:
+---------+-----------------------------------------+---------+---------+
| TYPE    | PATH                                    | STATE   | SIZE    |
+---------+-----------------------------------------+---------+---------+
| DIR     | http://192.168.1.133/assets             | 301     | 236     |
| DIR     | http://192.168.1.133/components         | 301     | 240     |
| DIR     | http://192.168.1.133/css                | 301     | 233     |
| DIR     | http://192.168.1.133/db                 | 301     | 232     |
| DIR     | http://192.168.1.133/icon               | 301     | 234     |
| DIR     | http://192.168.1.133/js                 | 301     | 232     |
| DIR     | http://192.168.1.133/path               | 301     | 234     |
| DIR     | http://192.168.1.133/php                | 301     | 233     |
| DIR     | http://192.168.1.133/uploads            | 301     | 237     |
| DIR     | http://192.168.1.133/vendor             | 301     | 236     |
+---------+-----------------------------------------+---------+---------+

[+] Discovered Files:
+---------+-----------------------------------------+---------+---------+
| TYPE    | PATH                                    | STATE   | SIZE    |
+---------+-----------------------------------------+---------+---------+
| GIT/HEAD | http://192.168.1.133/.git/HEAD         | 200     | 23      |
| JSON    | http://192.168.1.133/composer.json      | 200     | 95      |
| HTML    | http://192.168.1.133/index.html         | 200     | 20925   |
| HTML    | http://192.168.1.133/index.html         | 200     | 20925   |
| JSON    | http://192.168.1.133/package.json       | 200     | 54      |
| TXT     | http://192.168.1.133/robots.txt         | 200     | 58      |
| TXT     | http://192.168.1.133/robots.txt         | 200     | 58      |
+---------+-----------------------------------------+---------+---------+

[+] Gobuster scanning log saved to: ../logs/gobuster/gobusterscan20250122_213241.log
```