

1.1 ~ 1.3 Kali, Web Server, OSSEC, Suricata를 설치하여 정상 동작이 가능하도록 하시오. (Kali, Web Server는 제외)

```

** Alert 1738834794.154: - pam,syslog,
2025 Feb 06 09:39:54 joserver->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
2025-02-06T09:39:54.631384+00:00 joserver sshd[1311]: pam_unix(sshd:session): session closed for user jo

** Alert 1738834794.396: - pam,syslog,
2025 Feb 06 09:39:54 joserver->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
2025-02-06T09:39:54.638489+00:00 joserver su[1380]: pam_unix(su:session): session closed for user root

** Alert 1738834794.636: - pam,syslog,
2025 Feb 06 09:39:54 joserver->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
2025-02-06T09:39:54.640374+00:00 joserver sudo: pam_unix(sudo:session): session closed for user root

^[[
** Alert 1738834816.874: - pam,syslog,authentication_failed,
2025 Feb 06 09:40:16 joserver->/var/log/auth.log
Rule: 5503 (level 5) -> 'User login failed.'
Src IP: 192.168.5.5
User: jo
2025-02-06T09:40:15.529496+00:00 joserver sshd[25433]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
=jo

** Alert 1738834818.1223: - syslog,sshd,authentication_failed,
2025 Feb 06 09:40:18 joserver->/var/log/auth.log
Rule: 5716 (level 5) -> 'SSHD authentication failed.'
Src IP: 192.168.5.5
User: jo
2025-02-06T09:40:17.578332+00:00 joserver sshd[25433]: Failed password for jo from 192.168.5.5 port 50851 ssh2

```

OSSEC 감지 정상 동작 화면

```

[root@localhost suricata]# suricata -V
This is Suricata version 7.0.8 RELEASE

```

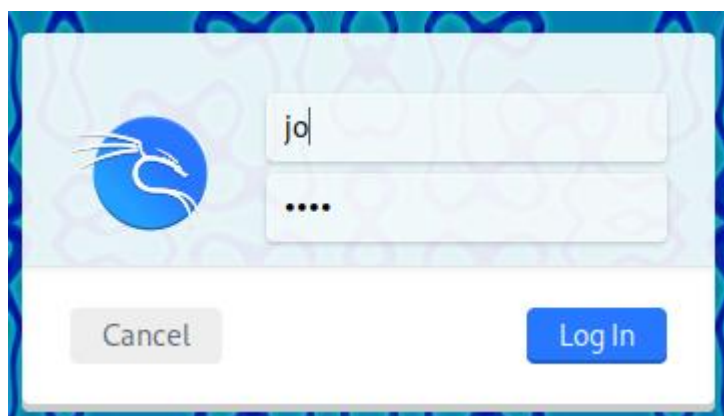
```

02/06/2025-01:25:59.423154  [**] [1:1000000:1] DDoS Attack [**] [Classification: (
null)] [Priority: 3] {ICMP} 192.168.5.109:8 -> 192.168.5.108:0

```

Suricata 감지 정상 동작 화면

1.4 Kali 시스템에 사용자(본인이름)를 추가하고 패스워드를 설정하도록 하시오.



```

(jo@kali-jo)-[~]
$

```

칼리 본인이름으로 로그인

2.1 ~ 2.5 Suricata Rule 을 정책 조건에 맞게 설정하고 탐지 테스트를 진행하시오.

HOST(Window) IP – 192.168.5.5

Suricata IP – 192.168.5.108

Kali IP – 192.168.5.109

WebServer IP – 192.168.5.110

OSSEC IP – 192.168.5.111

```
alert icmp 192.168.5.109 any -> $HOME_NET any (msg:"Kali-Suricata DDoS";sid:1000000;rev:1;)
)
alert tcp 192.168.5.109 any -> 192.168.5.110 80 (msg:"Kali-WebServer HTTP";sid:1000001;rev:1;)
)
alert tcp 192.168.5.5 any -> 192.168.5.110 23 (msg:"Host-WebServer Telnet";sid:1000002;rev:1;)
)
alert tcp 192.168.5.5 any -> 192.168.5.110 22 (msg:"Host-WebServer SSH";sid:1000003;rev:1;)
)
alert icmp 192.168.5.5 any -> 192.168.5.111 any (msg:"Host-OSSEC ICMP";sid:1000004;rev:1;)
)
```

Suricata rules 설정

1. Kali -> Suricata : DDoS 공격 탐지

```
02/06/2025-01:25:59.423154  [**] [1:1000000:1] DDoS Attack [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.5.109:8 -> 192.168.5.108:0
```

2. Kali -> Web Server : HTTP 접속 탐지

```
02/07/2025-00:05:39.396487  [**] [1:1000001:1] Kali-WebServer HTTP [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.5.109:48682 -> 192.168.5.110:80
```

3. Host(Windows) -> Web Server : Telnet 접속 탐지

```
02/07/2025-00:09:20.151025  [**] [1:1000002:1] Host-WebServer Telnet [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.5.5:49848 -> 192.168.5.110:23
```

4. Host(Windows) -> Web Server : ssh 접속 탐지

```
02/07/2025-00:11:38.686843  [**] [1:1000003:1] Host-WebServer SSH [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.5.5:49864 -> 192.168.5.110:22
```

5. Host(Windows) -> OSSEC : ICMP 패킷 탐지

```
02/07/2025-00:14:10.133192  [**] [1:1000004:1] Host-OSSEC ICMP [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.5.5:8 -> 192.168.5.111:0
```

2.6 위의 탐지되는 패킷들 중 Telnet 및 ssh 트래픽을 Wireshark로 캡처하여 스트림 분석을 통해 차이점을 확인하시오.


Wireshark · TCP 스트림 따라가기(tcp.stream eq 2) · 이더넷

```
.....#.....#.....X."
Kernel 5.14.0-503.22.1.el9_5.x86_64 on an x86_64
...localhost login: ...jjoo

Password: 1234

Last login: Fri Feb 7 00:46:32 from localhost
.[?2004h[jo@localhost ~]$
```

Telnet 분석 화면

 Wireshark · TCP 스트림 따라가기(tcp.stream eq 6) · 이더넷

```
SSH-2.0-PuTTY_Release_0.82
SSH-2.0-OpenSSH_8.7
...d..A.U..|.....
sntrup761x25519-sha512,sntrup761x25519-sha512@openssh.com,curve448-sha512,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group16-sha512,diffie-hellman-group17-sha512,diffie-hellman-group18-sha512,diffie-hellman-g
roup15-sha512,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,rsa2048-sha256,rsa1024-sha1,diffie-hellman-group1-sha1,ext-info-c,kex-strict-c-v00@openssh.com...{ssh-ed25
519,ssh-ed448,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,rsa-sha2-512,rsa-sha2-256,ssh-rsa,ssh-dss...aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ct
r,aes192-cbc,aes128-ctr,aes128-cbc,chacha20-poly1305@openssh.com,aes128-gcm@openssh.com,blowfish-ctr,blowfish-cbc,3des-ctr,3des-cbc,arcfour256,arcfour128..
aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,chacha20-poly1305@openssh.com,aes128-gcm@openssh.com,aes256-gcm@openssh.com,blowfi
sh-ctr,blowfish-cbc,3des-ctr,3des-cbc,arcfour256,arcfour128...hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh
.com,hmac-sha1-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-etm@openssh.com...hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-sha2-256-etm@openssh.com,
hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-etm@openssh.com...none,zlib@openssh.com...none,zlib@openssh.com.....
.....mV....."1.^v....curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256
,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,kex-strict-s-v00@openssh.com...9rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed255
19...aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr...aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes128-
gcm@openssh.com,aes128-ctr...hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha1,umac-128@open
ssh.com,hmac-sha2-512...none,zlib@openssh.com...none,zlib@openssh.com...?a...sTD.....H.....t.....3....ssh-ed25519.....
j"/3.Y.....N.....C.....qR.....W.M.R.5...Q.....S....ssh-ed25519...@jd...I.....K)...
w...E.3.8P...0fh.gK.8...n.NL...T...D.e.r...
.....jeD.V5.4.....@2:X.&.....@T...B...Z.....@K.../...W.Duf...c.bD...tk90...h.E...U.4...[d=...j...r1P.V|U...o...j.M.X...Wix$....A....z...[.W..f...6..
....QR~].U.....D...A~.1..P..5_K.j.z..|^.....N..b..
Z[...H....J*...C[.....cx....W.nE.S.qITn.
```

SSH 분석 화면

두 방법 분석 결과 Telnet은 보안성이 취약하여 아이디와 패스워드가 그대로 노출되는 반면 SSH는 암호화되
어 출력되기 때문에 보안에 더 강하다는 것을 알 수 있다.

3.1 ~ 3.4 OSSEC Agent 설정을 통해 Agent 시스템(Windows 또는 Linux)의 트래픽 현황 및 하드웨어 사용량을 실시간 모니터링을 통해 운영 및 현황을 파악할 수 있고 로그를 확인하시오.

```
Available agents:
  ID: 001, Name: jo, IP: 192.168.5.5
```

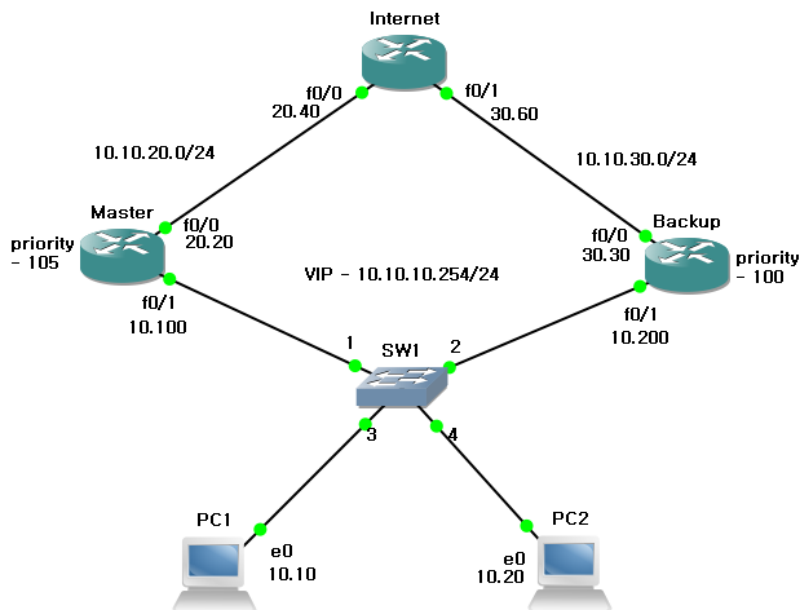
```
** Alert 1738908864.4302: - pam,syslog,authentication_success,
2025 Feb 07 06:14:24 joserver->/var/log/auth.log
Rule: 5501 (level 3) -> 'Login session opened.'
2025-02-07T06:14:23.108516+00:00 joserver su[1763]: pam_unix(su:session): session opened for user root(uid=0) by jo(uid=0)

** Alert 1738909136.4586: - pam,syslog,authentication_failed,
2025 Feb 07 06:18:56 joserver->/var/log/auth.log
Rule: 5503 (level 5) -> 'User login failed.'
Src IP: 192.168.5.5
User: jo
2025-02-07T06:18:55.369354+00:00 joserver sshd[1784]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.5.5 user=jo

** Alert 1738909138.4935: - syslog,sshd,authentication_failed,
2025 Feb 07 06:18:58 joserver->/var/log/auth.log
Rule: 5716 (level 5) -> 'SSHD authentication failed.'
Src IP: 192.168.5.5
User: jo
2025-02-07T06:18:57.263387+00:00 joserver sshd[1784]: Failed password for jo from 192.168.5.5 port 50427 ssh2
```

실시간 모니터링을 통해 이상이 있는 로그를 확인 (외부에서 putty로 원격 접속을 시도했으나 비밀번호 오류로 접근에 실패했다는 로그를 확인할 수 있음)

3.5 FHRP(First Hops Redundancy Protocol) 중에서 HSRP 를 통해 비정상 동작에 대응하기 위해 이중화를 설정하여 테스트를 진행하시오.



토폴로지

```
Master(config-if)#do sh standby brief
P indicates configured to preempt.
|
Interface Grp Pri P State Active Standby Virtual IP
Fa0/1 1 105 P Active local 10.10.10.200 10.10.10.254
```

이중화 세팅 상황(Master)

```
PC1> trace 10.10.30.60
trace to 10.10.30.60, 8 hops max, press Ctrl+C to stop
 1 *10.10.10.100 5.860 ms 8.781 ms
 2 *10.10.20.40 22.448 ms (ICMP type:3, code:3, Destination port unreachable)
)
```

(정상) PC1에서 10.10.30.60으로 보냈을 때

```
PC1> trace 10.10.30.60
trace to 10.10.30.60, 8 hops max, press Ctrl+C to stop
 1 10.10.10.200 6.826 ms 9.758 ms 9.758 ms
 2 *10.10.30.60 30.294 ms (ICMP type:3, code:3, Destination port unreachable)
)
```

(Master 라우터에 장애 발생 시) PC1에서 10.10.30.60으로 보냈을 때 - Backup 라우터로 돌아감