

보안위협 관리통제

문제해결 시나리오

악성코드분석 및 모의해킹 전문가 양성과정

김 다 승

차 례

| | |
|---|----------|
| 1. 보안위협 탐지하기 | ----- 3 |
| 1-1. 보안 요구사항 | ----- 3 |
| 1-2. 체크리스트 작성 | ----- 3 |
| 1-3. 보안 요구사항을 기반으로 IDS와 UTM 등의 보안 솔루션을 이용한 보안위협 관리통제시스템을 구축하라. | ----- 4 |
| 1-4. 모의해킹 후 기록된 로그 확인하기 | ----- 5 |
| 2. 보안위협 분석하기 | ----- 12 |
| 2-1. 수집 된 로그를 분석하여 공격의 종류와 공격 대상, 보안위협의 경로를 확인하기 | ----- 12 |
| 2-2. 탐지나 차단되지 않은 보안위협 대상의 취약한 원인과 영향도를 분석하기 | ----- 12 |
| 3. 보안위협 대응하기 | ----- 13 |
| 3-1. 보안위협에 대한 분석결과에 따라 확인 된 보안위협의 경로를 차단하기 | ----- 13 |
| 4. 사후처리하기 | ----- 20 |
| 4-1. 모의해킹 시 탐지나 차단되지 않은 보안위협에 대한 대응 결과를 보고하라. | ----- 20 |
| 4-2. 보완된 정보시스템의 보안설정을 최종 점검하고 취약점 발견 시 추가 대응책을 제시하라. | ----- 20 |

1. 보안위협 탐지하기

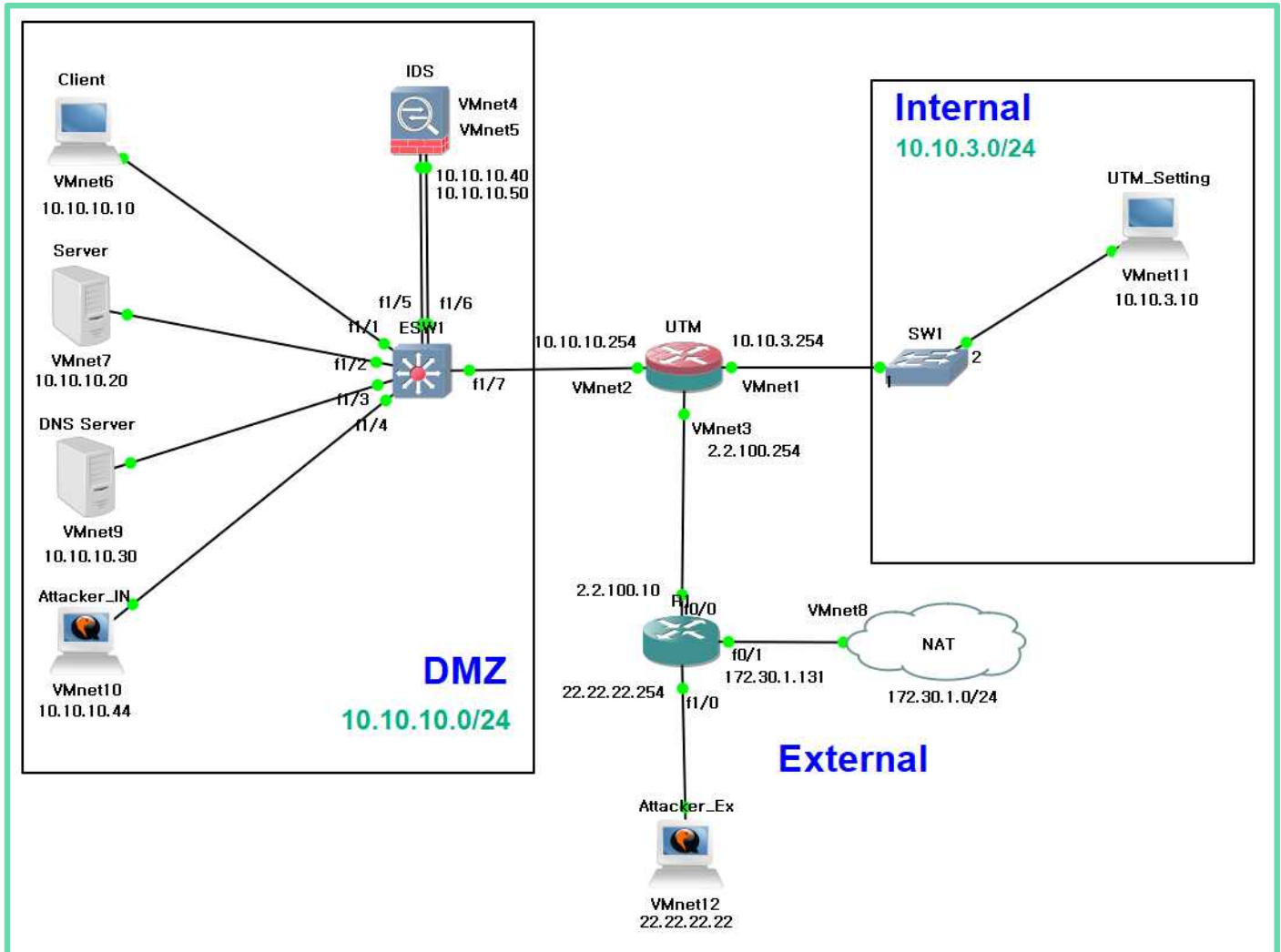
1-1. 보안 요구사항

- 가. MITM(Man In The Middle) 공격 탐지
- 나. Bruteforcing 공격 탐지
- 다. Port Scanning 탐지 및 차단
- 라. 외부 또는 내부로 부터의 웹 공격 탐지 및 차단
- 마. DoS(TCP flooding, UDP Flooding, ICMP Flooding) 공격 탐지 및 차단

1-2. 체크리스트 작성

| 취약점 | 확인 수단 |
|-------------------------|------------------|
| MITM(Man In The Middle) | ARP Spoofing |
| Bruteforcing | hydra |
| Port Scanning | nmap |
| 웹 공격 | XSS |
| | SQL Injection |
| DoS | TCP SYN Flooding |
| | UDP Flooding |
| | ICMP Flooding |

1-3. 보안 요구사항을 기반으로 IDS와 UTM 등의 보안 솔루션을 이용한 보안위협 관리통제시스템을 구축하라.



1) 내부 --> 내부

DMZ 부분에 공격자를 넣어놓고 내부에서 공격을 시도할 때마다 탐지하도록 설정

2) 외부 --> External

외부의 공격자가 UTM의 External IP를 통해서 웹 서버에 접근 및 공격 시도하면 탐지하도록 설정

1-4) 웹 공격

(1) XSS

> IDS

alert tcp any any -> any 80 (flags:PA; fragbits:D; msg:"XSS!!"; sid:1000002;)
/nsm/server_data/securityonion/rules/test-virtual-machine-eth0-1/local.rules: Line 2

| IP | Source IP | | Dest IP | | Ver | HL | TOS | len | ID | Flags | Offset | TTL | ChkSum |
|----|-------------|--|-------------|--|-----|----|-----|-----|------|-------|--------|-----|--------|
| | 10.10.10.10 | | 10.10.10.20 | | 4 | 5 | 0 | 685 | 1709 | 2 | 0 | 128 | 51564 |

| TCP | U A P R S F | | | | | | | | | | | | | | | | | | | | |
|-----|-------------|------|------|---|---|---|---|---|---|---|------------|---|------------|--|-------|---|--------|-----|--------|-----|--------|
| | Source | | Dest | | R | R | R | C | S | S | Y | I | Seq # | | Ack # | | Offset | Res | Window | Urp | ChkSum |
| | Port | Port | 1 | 0 | G | K | H | T | N | N | | | | | | | | | | | |
| | 1093 | 80 | . | . | . | X | X | . | . | . | 3693607579 | | 2604283528 | | 5 | 0 | 32768 | 0 | 51986 | | |

| DATA | 67 75 61 67 65 3A 20 6B 6F 2D 4B 52 2C 6B 6F 3B | guage: ko-KR,ko; q=0.8,en-US;q=0. 6,en;q=0.4..Cook ie: ASPSESSIONID CSRAAATR=LFBFEJO BJAABIHFCLKJDDFN J.... |
|------|---|---|
| | 71 3D 30 2E 38 2C 65 6E 2D 55 53 3B 71 3D 30 2E | |
| | 36 2C 65 6E 3B 71 3D 30 2E 34 0D 0A 43 6F 6F 6B | |
| | 69 65 3A 20 41 53 50 53 45 53 53 49 4F 4E 49 44 | |
| | 43 53 52 41 41 41 54 52 3D 4C 46 42 46 45 4A 4F | |
| | 42 4A 41 41 42 49 48 46 4B 4C 4B 4A 44 44 46 4E | |
| | 4A 0D 0A 0D 0A | |

(2) SQL Injection

> IDS

| ST | CNT | Sensor | Alert ID | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|----|-----|---------------|----------|---------------------|-------------|-------|-------------|-------|----|---------------------------|
| RT | 1 | test-virtu... | 3.42674 | 2020-01-19 13:24:44 | 10.10.10.44 | 49688 | 10.10.10.20 | 80 | 6 | Snort Alert [1:1000001:0] |

| IP Resolution | Agent Status | Snort Statistics | System Msgs |
|--------------------------------------|---|------------------------------|------------------------------|
| <input type="checkbox"/> Reverse DNS | <input checked="" type="checkbox"/> Enable External DNS | | |
| Src IP: | | | |
| Src Name: | | | |
| Dst IP: | | | |
| Dst Name: | | | |
| Whois Query: | <input checked="" type="radio"/> None | <input type="radio"/> Src IP | <input type="radio"/> Dst IP |

| Show Packet Data | | Show Rule | |
|---|--|-----------|--|
| alert tcp any any -> any 80 (msg:"ADMIN INJECTION!!!"; flags:PA; fragbits:D; resp:rst_snd; content:"POST"; http_method; uricontent:"/admin/admin_login.asp"; pcre:"/(and) ((and%20) (or) ((or%20) (or')) (select) (from) (where) (substring) (union) (delete) (\' (\%27) (\#) (\%23) (\%5C) (\%00))"; nocase; sid:1000001;) | | | |
| /nsm/server_data/securityonion/rules/test-virtual-machine-eth0-1/local.rules: Line 1 | | | |

| IP | Source IP | Dest IP | Ver | HL | TOS | len | ID | Flags | Offset | TTL | ChkSum |
|----|-------------|-------------|-----|----|-----|-----|------|-------|--------|-----|--------|
| | 10.10.10.44 | 10.10.10.20 | 4 | 5 | 0 | 618 | 3242 | 2 | 0 | 64 | 913 |

| TCP | Source Port | Dest Port | R | R | R | C | S | S | Y | I | Seq # | Ack # | Offset | Res | Window | Urp | ChkSum |
|-----|-------------|-----------|---|---|---|---|---|---|---|---|------------|------------|--------|-----|--------|-----|--------|
| | 49688 | 80 | . | . | . | X | X | . | . | . | 2597173638 | 2291038457 | 8 | 0 | 913 | 0 | 4996 |

| DATA | 6C 3D 2F 69 6E 64 65 78 2E 61 73 70 0D 0A 43 6F | 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49 4F 4E | 49 44 43 43 42 43 44 42 42 44 3D 45 44 43 41 4E | 4C 45 41 50 43 42 47 4A 4D 4F 45 4A 4B 50 4B 45 | 4A 49 41 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 | 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 | 2D 77 77 77 2D 66 6F 72 6D 2D 75 72 6C 65 6E 63 | 6F 64 65 64 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 | 6E 67 74 68 3A 20 38 35 0D 0A 48 6F 73 74 3A 20 | 77 77 77 2E 63 61 6D 65 6C 2E 63 6F 6D 0D 0A 0D | 0A 61 64 6D 69 6E 5F 69 64 3D 31 25 32 37 6F 72 | 25 32 37 31 25 32 37 25 33 44 25 32 37 31 26 61 | 64 6D 69 6E 5F 70 61 73 73 3D 31 25 32 37 6F 72 | 25 32 37 31 25 32 37 25 33 44 25 32 37 31 26 53 | 75 62 6D 69 74 32 32 32 3D 25 43 38 25 41 45 | 25 43 30 25 43 45 |
|------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|--|-------------------|
| | l=/index.asp..Co okie: ASPSESSION IDCCBCDBBD=EDCAN LEAPCBGJMOEJKPKE JIA..Content-Typ e: application/x -www-form-urlencoded..Content-Le ngth: 85..Host: www.camel.com... .admin_id=1%27or %271%27%3D%271&a dmin_pass=1%27or %271%27%3D%271&S ubmit2222=%C8%AE %C0%CE | | | | | | | | | | | | | | | |

1-5) DoS

(1) TCP Flooding

> IDS

| ST | CNT | Sensor | Alert ID | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|----|------|---------------|----------|---------------------|-------------|-------|-------------|-------|----|---------------------------|
| RT | 1260 | test-virtu... | 3.42696 | 2020-01-19 15:25:56 | 10.10.10.44 | 2463 | 10.10.10.20 | 23 | 6 | Snort Alert [1:1000001:0] |

IP Resolution Agent Status Snort Statistics **System Ms**

☐ Reverse DNS ☒ Enable External DNS

Src IP:
Src Name:

Dst IP:
Dst Name:

Whois Query: ☒ None ☐ Src IP ☐ Dst IP

☒ Show Packet Data ☒ Show Rule
alert tcp any any -> any 23 (msg:"SYN Flooding!!"; flags:S; threshold:type threshold, track by_src, count 10, seconds 1; sid:1000001;)
/nsm/server_data/securityonion/rules/test-virtual-machine-eth0-1/local.rules: Line 1

| IP | Source IP | Dest IP | Ver | HL | TOS | len | ID | Flags | Offset | TTL | hkSum |
|----|-------------|-------------|-----|----|-----|-----|-------|-------|--------|-----|-------|
| | 10.10.10.44 | 10.10.10.20 | 4 | 5 | 0 | 40 | 54832 | 0 | 0 | 64 | 318 |

| TCP | Source Port | Dest Port | Seq # | Ack # | Offset | Res Window | Urp | hkSum |
|-----|-------------|-----------|-----------|-----------|--------|------------|-----|-------|
| | 2463 | 23 | 181433868 | 748974169 | 5 | 0 | 512 | 0 |

None.

None.

(2) UDP Flooding

> IDS

| ST | CNT | Sensor | Alert ID | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|----|-----|---------------|----------|---------------------|-------------|-------|-------------|-------|----|---------------------------|
| RT | 261 | test-virtu... | 3.44173 | 2020-01-19 15:43:42 | 10.10.10.44 | 2924 | 10.10.10.20 | 0 | 17 | Snort Alert [1:1000001:0] |

IP Resolution Agent Status Snort Statistics **System Ms**

☐ Reverse DNS ☒ Enable External DNS

Src IP:
Src Name:

Dst IP:
Dst Name:

Whois Query: ☒ None ☐ Src IP ☐ Dst IP

☒ Show Packet Data ☒ Show Rule
alert udp any any -> any any (msg:"UDP Flooding!!"; threshold:type threshold, track by_dst, count 10, seconds 1; sid:1000001;)
/nsm/server_data/securityonion/rules/test-virtual-machine-eth0-1/local.rules: Line 1

| IP | Source IP | Dest IP | Ver | HL | TOS | len | ID | Flags | Offset | TTL | hkSum |
|----|-------------|-------------|-----|----|-----|-----|-------|-------|--------|-----|-------|
| | 10.10.10.44 | 10.10.10.20 | 4 | 5 | 0 | 28 | 50719 | 0 | 0 | 64 | 359 |

| UDP | Source Port | Dest Port | Length | ChkSum |
|-----|-------------|-----------|--------|--------|
| | 2924 | 0 | 8 | 52254 |

None.

None.

(3) ICMP Flooding

> IDS

alert icmp any any -> 10.10.10.20/24 any (itype:8; msg:"ICMP Flooding!!"; threshold:type both, track by_dst, count 10, seconds 1; sid:1000002;)
/nsm/server_data/securityonion/rules/test-virtual-machine-eth0-1/local.rules: Line 2

| IP | Source IP | Dest IP | Ver | HL | TOS | len | ID | Flags | Offset | TTL | ChkSum |
|----|-------------|-------------|-----|----|-----|-----|-------|-------|--------|-----|--------|
| | 10.10.10.44 | 10.10.10.20 | 4 | 5 | 0 | 28 | 44451 | 0 | 0 | 64 | 42218 |

| ICMP | Type | Code | ChkSum | ID | Seq # |
|------|------|------|--------|------|-------|
| | 8 | 0 | 47550 | 1800 | 14137 |

| DATA |
|-------|
| None. |

2) 외부 --> External

- 외부에서 External의 ip를 통해 웹 서버로 통하는 경우 IDS가 탐지하지만 단지 External의 ip 단독공격일 경우 IDS가 탐지하지 못한다.

2-1) MITM : 탐지 불가

(1) ARP Spoofing

2-1) Bruteforcing

(1) hydra

> IDS

```
alert tcp any any -> any any (msg:"bruteforcing!!"; content:"POST"; http_method;flow:established,to_server; uricontent:"/login/login_chk.asp"; nocase;
threshold:type both, track by_dst, count 10, seconds 1; sid:1000003;)
/nsm/server_data/securityonion/rules/test-virtual-machine-eth0-1/local.rules: Line 3
```

| IP | Source IP | | | | Dest IP | | | | Ver | HL | TOS | len | ID | Flags | Offset | TTL | ChkSum |
|---|---|-----------|-----|-----|-------------|-----|-----|-----|-----|-------|------------|------------------|------------------|-------|--------|-----|--------|
| | 10.10.10.254 | | | | 10.10.10.20 | | | | 4 | 5 | 0 | 431 | 29608 | 2 | 0 | 64 | 40059 |
| TCP | U A P R S F | | | | | | | | | | | | | | | | |
| | Source Port | Dest Port | R 1 | R 0 | U G | A C | P S | R S | Y I | Seq # | | Ack # | Offset | Res | Window | Urp | ChkSum |
| | 53046 | 80 | . | . | . | X | X | . | . | . | 2857148659 | 3798889090 | 8 | 0 | 229 | 0 | 58897 |
| DATA | 42 41 41 54 52 3D 4A 4A 50 49 42 4B 50 44 41 4E | | | | | | | | | | | | BAATR=JJPIBKPDAN | | | | |
| | 4D 4D 4B 41 42 41 41 46 45 47 41 44 46 48 0D 0A | | | | | | | | | | | | MMKABAAFEGADFH.. | | | | |
| | 58 2D 46 6F 72 77 61 72 64 65 64 2D 50 72 6F 74 | | | | | | | | | | | | X-Forwarded-Prot | | | | |
| | 6F 3A 20 68 74 74 70 0D 0A 58 2D 46 6F 72 77 61 | | | | | | | | | | | | o: http..X-Forwa | | | | |
| | 72 64 65 64 2D 46 6F 72 3A 20 32 32 2E 32 32 2E | | | | | | | | | | | | rded-For: 22.22. | | | | |
| | 32 32 2E 32 32 0D 0A 58 2D 46 6F 72 77 61 72 64 | | | | | | | | | | | | 22.22..X-Forward | | | | |
| | 65 64 2D 48 6F 73 74 3A 20 32 2E 32 2E 31 30 30 | | | | | | | | | | | | ed-Host: 2.2.100 | | | | |
| | 2E 32 35 34 0D 0A 58 2D 46 6F 72 77 61 72 64 65 | | | | | | | | | | | | .254..X-Forwarde | | | | |
| | 64 2D 53 65 72 76 65 72 3A 20 32 2E 32 2E 31 30 | | | | | | | | | | | | d-Server: 2.2.10 | | | | |
| | 30 2E 32 35 34 0D 0A 43 6F 6E 6E 65 63 74 69 6F | | | | | | | | | | | | 0.254..Connectio | | | | |
| | 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A 43 | | | | | | | | | | | | n: Keep-Alive..C | | | | |
| | 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 32 | | | | | | | | | | | | ontent-Length: 2 | | | | |
| 32 0D 0A 0D 0A 69 64 3D 74 65 73 74 26 70 61 73 | | | | | | | | | | | | 2....id=test&pas | | | | | |
| 73 3D 70 61 73 73 77 6F 72 64 31 | | | | | | | | | | | | s=password1 | | | | | |

> UTM

- Post, Get 순으로 출력된다

```
2020:01:23-03:32:54 test httpd: id="0299" srcip="22.22.22.22" localip="2.2.100.254" size="127"
user="-" host="22.22.22.22" method="POST" statuscode="302" reason="-" extra="-" exceptions
="-" time="5977" url="/login/login_chk.asp" server="2.2.100.254" port="80" query="" referer="-"
cookie="ASPSESSIONIDCCCBAATR=LMBJBKPDJBCAMGCGCGJKNLKL" set-cookie="-" uid="XiiV
VgICZP4AAG5rrx4AAAAI"
```

```
2020:01:23-03:32:54 test httpd: id="0299" srcip="22.22.22.22" localip="2.2.100.254" size="45589"
user="-" host="22.22.22.22" method="GET" statuscode="200" reason="-" extra="-" exceptions
="-" time="41717" url="/index.asp" server="2.2.100.254" port="80" query="" referer="-" cookie=
"ASPSESSIONIDCCCBAATR=LMBJBKPDJBCAMGCGCGJKNLKL" set-cookie="-" uid="XiiVVgICZP4
AAG5rrx8AAAAr"
```


2-2) Port Scanning

> IDS : 탐지 불가

> UTM

2020:01:23-03:27:00 test ulogd[12611]: id="2102" severity="info" sys="SecureNet" sub="ips" name="portscan detected" action="portscan" fwrule="60017" initf="eth2" srcmac="cc:01:0b:b4:00:00" dstmac="00:0c:29:22:bc:60" srcip="22.22.22.22" dstip="2.2.100.254" proto="6" length="44" tos="0x00" prec="0x00" ttl="52" srcport="51955" dstport="587" tcpflags="SYN"

2-3) 웹 공격

(1) XSS

> IDS

alert tcp any any -> any 80 (flags:PA; fragbits:D; resp:rst_snd; msg:"XSS!!"; sid:1000002;)
/nsm/server_data/securityonion/rules/test-virtual-machine-eth0-1/local.rules: Line 2

| IP | Source IP | Dest IP | Ver | HL | TOS | len | ID | Flags | Offset | TTL | hkSul |
|------|--|-------------|--------|-----|--------|-----|-------|-------|--------|-----|-------|
| | 10.10.10.10 | 10.10.10.20 | 4 | 5 | 0 | 757 | 4216 | 2 | 0 | 128 | 489 |
| TCP | Source Port | Dest Port | R | R | R | C | S | S | Y | I | |
| | 1434 | 80 | . | . | . | X | X | . | . | . | |
| | Seq # | Ack # | Offset | Res | Window | Urp | hkSul | | | | |
| | 2334242103 | 445986651 | 5 | 0 | 64240 | 0 | 249 | | | | |
| DATA | <pre> 31 30 32 32 29 0D 0A 41 03 03 03 70 74 2D 43 0E ection: keep-al 63 6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20 64 65 i 66 6C 61 74 65 0D 0A 48 6F 73 74 3A 20 77 77 77 ve..Cookie: ASP 2E 63 61 6D 65 6C 2E 63 6F 6D 0D 0A 43 6F 6E 6E S 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 ESSIONIDCSRAAAT 76 65 0D 0A 43 6F 6F 6B 69 65 3A 20 41 53 50 53 R 45 53 53 49 4F 4E 49 44 43 53 52 41 41 41 54 52 =JFCFEJOBPCAEJ 3D 4A 46 43 46 45 4A 4F 42 50 43 41 45 45 4A 4C L 4C 43 41 4D 4B 42 4C 46 45 0D 0A 0D 0A LCAMKBLFE.... </pre> | | | | | | | | | | |

> UTM : 탐지 불가

공격대상이 공격자의 IP로 패킷을 보내는 것은 확인이 되나 해당 패킷이 XSS에 의해 발생된 패킷이라는 탐지는 못함.

(2) SQL Injection

> IDS

| IP | Source IP | | | | Dest IP | | | | Ver | HL | TOS | len | ID | Flags | Offset | TTL | ChkSum | | | | | | | | | | | |
|--|---|--|--|--|-------------|--|--|--|-----|-----|-------|---------|---------|---------|--------|-------|------------|------------------|------------------|--------|-----|--------|-------|--|--|--|--|--|
| | 10.10.10.254 | | | | 10.10.10.20 | | | | 4 | 5 | 0 | 727 | 47433 | 2 | 0 | 64 | 21938 | | | | | | | | | | | |
| TCP | Source Port | | | | Dest Port | | | | R 1 | R 0 | U R G | A R C K | P S S H | T S Y N | F I N | Seq # | Ack # | Offset | Res | Window | Urp | ChkSum | | | | | | |
| | 53363 | | | | 80 | | | | . | . | . | X | X | . | . | . | 3304395461 | 4166016355 | 8 | 0 | 229 | 0 | 14386 | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DATA | 49 4F 4E 49 44 43 43 43 42 41 41 54 52 3D 4F 43 | | | | | | | | | | | | | | | | | | IONIDCCCBAATR=OC | | | | | | | | | |
| | 41 4A 42 4B 50 44 4B 50 41 49 4C 4F 41 49 47 4F | | | | | | | | | | | | | | | | | | AJBKPKPAILOAIGO | | | | | | | | | |
| | 49 4F 4C 46 4C 41 0D 0A 43 6F 6E 74 65 6E 74 2D | | | | | | | | | | | | | | | | | | IOLFLA..Content- | | | | | | | | | |
| | 54 79 70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F | | | | | | | | | | | | | | | | | | Type: applicatio | | | | | | | | | |
| | 6E 2F 78 2D 77 77 77 2D 66 6F 72 6D 2D 75 72 6C | | | | | | | | | | | | | | | | | | n/x-www-form-url | | | | | | | | | |
| | 65 6E 63 6F 64 65 64 0D 0A 58 2D 46 6F 72 77 61 | | | | | | | | | | | | | | | | | | encoded..X-Forwa | | | | | | | | | |
| | 72 64 65 64 2D 50 72 6F 74 6F 3A 20 68 74 74 70 | | | | | | | | | | | | | | | | | | rded-Proto: http | | | | | | | | | |
| | 0D 0A 58 2D 46 6F 72 77 61 72 64 65 64 2D 46 6F | | | | | | | | | | | | | | | | | | ..X-Forwarded-Fo | | | | | | | | | |
| | 72 3A 20 32 32 2E 32 32 2E 32 32 2E 32 32 0D 0A | | | | | | | | | | | | | | | | | | r: 22.22.22.22.. | | | | | | | | | |
| | 58 2D 46 6F 72 77 61 72 64 65 64 2D 48 6F 73 74 | | | | | | | | | | | | | | | | | | X-Forwarded-Host | | | | | | | | | |
| | 3A 20 32 2E 32 2E 31 30 30 2E 32 35 34 0D 0A 58 | | | | | | | | | | | | | | | | | | : 2.2.100.254..X | | | | | | | | | |
| | 2D 46 6F 72 77 61 72 64 65 64 2D 53 65 72 76 65 | | | | | | | | | | | | | | | | | | -Forwarded-Serve | | | | | | | | | |
| | 72 3A 20 32 2E 32 2E 31 30 30 2E 32 35 34 0D 0A | | | | | | | | | | | | | | | | | | r: 2.2.100.254.. | | | | | | | | | |
| | 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 | | | | | | | | | | | | | | | | | | Connection: Keep | | | | | | | | | |
| | 2D 41 6C 69 76 65 0D 0A 43 6F 6E 74 65 6E 74 2D | | | | | | | | | | | | | | | | | | -Alive..Content- | | | | | | | | | |
| | 4C 65 6E 67 74 68 3A 20 38 35 0D 0A 0D 0A 61 64 | | | | | | | | | | | | | | | | | | Length: 85....ad | | | | | | | | | |
| | 6D 69 6E 5F 69 64 3D 31 25 32 37 6F 72 25 32 37 | | | | | | | | | | | | | | | | | | min_id=1%27or%27 | | | | | | | | | |
| | 31 25 32 37 25 33 44 25 32 37 31 26 61 64 6D 69 | | | | | | | | | | | | | | | | | | 1%27%3D%271&admi | | | | | | | | | |
| | 6E 5F 70 61 73 73 3D 31 25 32 37 6F 72 25 32 37 | | | | | | | | | | | | | | | | | | n_pass=1%27or%27 | | | | | | | | | |
| | 31 25 32 37 25 33 44 25 32 37 31 26 53 75 62 6D | | | | | | | | | | | | | | | | | | 1%27%3D%271&Subm | | | | | | | | | |
| 69 74 32 32 32 3D 25 43 38 25 41 45 25 43 30 | | | | | | | | | | | | | | | | | | it2222=%C8%AE%CO | | | | | | | | | | |
| 25 43 45 | | | | | | | | | | | | | | | | | | %CE | | | | | | | | | | |

> UTM

2020:01:23-03:29:04 test httpd[28267]: [security2:error] [pid 28267:tid 2688248688] [client 2.22.22.22] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/apache/conf/waf/modsecurity_crs_correlation.conf"] [line "37"] [id "981204"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 46, SQLi=26, XSS=): 981242-Detects classic SQL injection probings 1/2"] [hostname "2.2.100.254"] [uri "/admin/admin_login.asp"] [unique_id "XiiUcAICZP4AAG5rrbwAAAAAs"]

2-4) DoS

(1) TCP SYN Flooding

> IDS : 탐지불가

> UTM

2020:01:23-03:18:58 test ulogd[12611]: id="2103" severity="info" sys="SecureNet" sub="ips" name="SYN flood detected" action="SYN flood" fwrule="60012" initf="eth2" srcmac="cc:01:0b:b4:00:00" dstmac="00:0c:29:22:bc:60" srcip="22.22.22.22" dstip="2.2.100.254" proto="6" length="40" tos="0x00" prec="0x00" ttl="63" srcport="38190" dstport="0" tcpflags="SYN"

(2) UDP Flooding

> IDS

| IP | Source IP | Dest IP | Ver | HL | TOS | len | ID | Flags | Offset | TTL | ChkSum | |
|---|---|-----------------|-----------|----|--------|-----|----------------|------------------|--------|-----|--------|--|
| | 192.168.72.1 | 239.255.255.250 | 4 | 5 | 0 | 202 | 57783 | 0 | 0 | 1 | 57031 | |
| UDP | Source Port | | Dest Port | | Length | | | | ChkSum | | | |
| | 58760 | | 1900 | | 182 | | | | 5173 | | | |
| DATA | 4D 2D 53 45 41 52 43 48 20 2A 20 48 54 50 2F | | | | | | | M-SEARCH * HTTP/ | | | | |
| | 31 2E 31 0D 0A 48 4F 53 54 3A 20 32 33 39 2E 32 | | | | | | | 1.1..HOST: 239.2 | | | | |
| | 35 35 2E 32 35 35 2E 32 35 30 3A 31 39 30 30 0D | | | | | | | 55.255.250:1900. | | | | |
| | 0A 4D 41 4E 3A 20 22 73 73 64 70 3A 64 69 73 63 | | | | | | | .MAN: "ssdp:disc | | | | |
| | 6F 76 65 72 22 0D 0A 4D 58 3A 20 31 0D 0A 53 54 | | | | | | | over"..MX: 1..ST | | | | |
| | 3A 20 75 72 6E 3A 64 69 61 6C 2D 6D 75 6C 74 69 | | | | | | | : urn:dial-multi | | | | |
| | 73 63 72 65 65 6E 2D 6F 72 67 3A 73 65 72 76 69 | | | | | | | screen-org:servi | | | | |
| | 63 65 3A 64 69 61 6C 3A 31 0D 0A 55 53 45 52 2D | | | | | | | ce:dial:1..USER- | | | | |
| | 41 47 45 4E 54 3A 20 47 6F 6F 67 6C 65 20 43 68 | | | | | | | AGENT: Google Ch | | | | |
| | 72 6F 6D 65 2F 37 39 2E 30 2E 33 39 34 35 2E 31 | | | | | | | rome/79.0.3945.1 | | | | |
| 33 30 20 57 69 6E 64 6F 77 73 0D 0A 0D 0A | | | | | | | 30 Windows.... | | | | | |

> UTM

2020:01:23-03:15:37 test ulogd[12611]: id="2105" severity="info" sys="SecureNet" sub="ips" name="UDP flood detected" action="UDP flood" fwrule="60013" initf="eth2" srcmac="cc:01:0b:b4:00:00" dstmac="00:0c:29:22:bc:60" srcip="22.22.22.22" dstip="2.2.100.254" proto="17" length="28" tos="0x00" prec="0x00" ttl="63" srcport="9216" dstport="0"

(3) ICMP Flooding

> IDS : 탐지불가

> UTM

2020:01:23-03:13:50 test ulogd[12611]: id="2104" severity="info" sys="SecureNet" sub="ips" name="ICMP flood detected" action="ICMP flood" fwrule="60014" initf="eth2" srcmac="cc:01:0b:b4:00:00" dstmac="00:0c:29:22:bc:60" srcip="22.22.22.22" dstip="2.2.100.254" proto="1" length="28" tos="0x00" prec="0x00" ttl="63" type="8" code="0"

2. 보안위협 분석하기

2-1. 수집 된 로그를 분석하여 공격의 종류와 공격 대상, 보안위협의 경로를 확인하기

| 공격 종류 | 공격 대상 | 보안위협의 경로 |
|---------------------|---------------------------|---------------------------|
| MITM - ARP Spoofing | 10.10.10.20 / 2.2.100.254 | 10.10.10.44 / 22.22.22.22 |
| Bruteforcing | 10.10.10.20 / 2.2.100.254 | 10.10.10.44 / 22.22.22.22 |
| Port Scanning | 10.10.10.20 / 2.2.100.254 | 10.10.10.44 / 22.22.22.22 |
| XSS | 10.10.10.20 / 2.2.100.254 | 10.10.10.44 / 22.22.22.22 |
| SQL Injection | 10.10.10.20 / 2.2.100.254 | 10.10.10.44 / 22.22.22.22 |
| TCP SYN Flooding | 10.10.10.20 / 2.2.100.254 | 10.10.10.44 / 22.22.22.22 |
| UDP Flooding | 10.10.10.20 / 2.2.100.254 | 10.10.10.44 / 22.22.22.22 |
| ICMP Flooding | 10.10.10.20 / 2.2.100.254 | 10.10.10.44 / 22.22.22.22 |

2-2. 탐지나 차단되지 않은 보안위협 대상의 취약한 원인과 영향도를 분석하기

| 공격 종류 | 취약한 원인 | 영향도 |
|------------------|----------------|-----------------|
| ARP Spoofing | ARP 변경 | 개인정보 및 입력값 노출 |
| Bruteforcing | 제한을 두지 않은 기회 | 개인정보 노출 |
| Port Scanning | 열려진 포트 | 열린 포트 및 취약점노출 |
| XSS | asp 파일의 취약점 파악 | 개인정보 노출 |
| SQL Injection | 보안상의 허점 | 개인정보 노출 및 보안 취약 |
| TCP SYN Flooding | 과부하로 인한 서비스거부 | 서버 접속 불가 |
| UDP Flooding | 과부하로 인한 서비스거부 | 서버 접속 불가 |
| ICMP Flooding | 과부하로 인한 서비스거부 | 서버 접속 불가 |

3. 보안위협 대응하기

3-1. 보안위협에 대한 분석결과에 따라 확인 된 보안위협의 경로를 차단하기

1) MITM

(1) ARP Spoofing : arp를 동적에서 정적으로 변경한다.

> 배치파일로 변경하면 영구적이다.

```
C:\>arp -a

Interface: 10.10.10.20 on Interface 0x1000003
    Internet Address      Physical Address      Type
    10.10.10.10           00-0c-29-b8-37-ab    dynamic
    10.10.10.254          00-0c-29-b8-37-ab    static

C:\>arp -s 10.10.10.254 00-0c-29-22-bc-56

C:\>arp -a

Interface: 10.10.10.20 on Interface 0x1000003
    Internet Address      Physical Address      Type
    10.10.10.10           00-0c-29-b8-37-ab    dynamic
    10.10.10.254          00-0c-29-22-bc-56    static
```


2) Bruteforcing

(1) hydra

(1-1) camel 속성 추가하기

```
use camel

select * from member

alter table member add incorrect_count int default 0 with values

update member set incorrect_count=0
where mem_id=' '
```

| incorrect_count |
|-----------------|
| 0 |
| 0 |

(1-2) 패스워드 불일치 시, 변수를 사용하여 제한시키기

```
if Rs("mem_pwd") <> pw then '패스워드 불일치
    sql = " update member set incorrect_count = incorrect_count+1 where mem_id='&id&' "
    db.execute(sql)
%>
    <script language="javascript">
        alert("비밀번호가 일치하지 않습니다. #다시한번 확인하여 주십시오.");
        location.replace("<%=local%>/login/login.asp?ba=search")
    </script>
<%
    Response.End
end if

if Rs("incorrect_count") >= 5 then
%>
    <script language = "javascript">
        alert("계정이 잠금되었습니다.#");
        location.replace("<%=local%>/login/login.asp?ba=search")
    </script>
<%
    Response.End
end if
```

(1-3) 공격 시도 및 차단 시도

```
root@bt:~# hydra 10.10.10.20 -l test100 -P passwords.txt http-post-form "/login/
login_chk.asp:id=^USER^&pass=^PASS^:login.asp" -f
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2020-01-21 17:12:04
[DATA] 16 tasks, 1 server, 265 login tries (l:1/p:265), ~16 tries per task
[DATA] attacking service http-post-form on port 80
[STATUS] attack finished for 10.10.10.20 (waiting for children to finish)
1 of 1 target successfully completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-01-21 17:12:07
```

3) XSS

(1-1) board_view.asp 내용 수정

```
if (rs("info_content") <> NULL) or (rs("info_content")<> "") then
    info_content = replace(rs("info_content"),chr(13) & chr(10),"<br>")
    info_content = replace(info_content "&")
    info_content = replace(info_content,"/</g","&lt;")
    info_content = replace(info_content,"/>/g","&gt;")
    info_content = replace(info_content, "/script/g","")
else
    info_content = ""
end if
```

(1-2) 차단 시도

| | | |
|---|------------------|--------|
| 작성자 : itbank | 작성일 : 2020.01.20 | 방문 : 5 |
| 제목 : 1 | | |
| <div><script>alert("XSS");</script></div> | | |

| | | |
|---|------------------|--------|
| 작성자 : 테스트 | 작성일 : 2020.01.21 | 방문 : 1 |
| 제목 : 2 | | |
| <div><<script>>alert("XSS");<</script>></div> | | |
| [다음글] 다음글이 없습니다 | | |
| [이전글] 1 | | |

| | | |
|---|------------------|--------|
| 작성자 : 테스트 | 작성일 : 2020.01.21 | 방문 : 1 |
| 제목 : 3 | | |
| <div><<scriptipt> alert("XSS");<<scriptipt>></div> | | |

4) Port scanning

(1) nmap

(1-1) Windows는 netstat -o 옵션이 있다면

PID를 확인하여 특정 PID로 활성화된 포트를 닫을 수 있다.

```
C:\Documents and Settings\Administrator>netstat -ano
```

Active Connections

| Proto | Local Address | Foreign Address | State | PID |
|-------|------------------|-----------------|-----------|------|
| TCP | 0.0.0.0:135 | 0.0.0.0:0 | LISTENING | 952 |
| TCP | 0.0.0.0:445 | 0.0.0.0:0 | LISTENING | 4 |
| TCP | 10.10.10.10:139 | 0.0.0.0:0 | LISTENING | 4 |
| TCP | 127.0.0.1:1029 | 0.0.0.0:0 | LISTENING | 1108 |
| UDP | 0.0.0.0:445 | *** | | 4 |
| UDP | 0.0.0.0:500 | *** | | 704 |
| UDP | 0.0.0.0:1025 | *** | | 1096 |
| UDP | 0.0.0.0:4500 | *** | | 704 |
| UDP | 10.10.10.10:123 | *** | | 1040 |
| UDP | 10.10.10.10:137 | *** | | 4 |
| UDP | 10.10.10.10:138 | *** | | 4 |
| UDP | 10.10.10.10:1033 | *** | | 1040 |
| UDP | 10.10.10.10:1900 | *** | | 1188 |
| UDP | 127.0.0.1:123 | *** | | 1040 |
| UDP | 127.0.0.1:1034 | *** | | 1040 |
| UDP | 127.0.0.1:1035 | *** | | 1040 |
| UDP | 127.0.0.1:1900 | *** | | 1188 |

```
C:\Documents and Settings\Administrator>taskkill /f /pid 1108
성공: 프로세스(PID 1108)가 종료되었습니다.
```

```
C:\Documents and Settings\Administrator>netstat -ano
```

Active Connections

| Proto | Local Address | Foreign Address | State | PID |
|-------|------------------|-----------------|-----------|------|
| TCP | 0.0.0.0:135 | 0.0.0.0:0 | LISTENING | 952 |
| TCP | 0.0.0.0:445 | 0.0.0.0:0 | LISTENING | 4 |
| TCP | 10.10.10.10:139 | 0.0.0.0:0 | LISTENING | 4 |
| UDP | 0.0.0.0:445 | *** | | 4 |
| UDP | 0.0.0.0:500 | *** | | 704 |
| UDP | 0.0.0.0:1025 | *** | | 1096 |
| UDP | 0.0.0.0:4500 | *** | | 704 |
| UDP | 10.10.10.10:123 | *** | | 1040 |
| UDP | 10.10.10.10:137 | *** | | 4 |
| UDP | 10.10.10.10:138 | *** | | 4 |
| UDP | 10.10.10.10:1900 | *** | | 1188 |
| UDP | 127.0.0.1:123 | *** | | 1040 |
| UDP | 127.0.0.1:1035 | *** | | 1040 |
| UDP | 127.0.0.1:1900 | *** | | 1188 |

(1-2) flooding 공격 방지로 레지스트리 편집기에 값 추가하는 방법도 있다.

> flooding 부분에서 레지스트리 값을 추가하는 내용이 있습니다.

(1-3) 외부로부터의 flooding 방지

Portscan detection



Global Settings

Action: Drop traffic

☒ Limit logging

Anti-Portscan can detect and optionally block port scans. The **Action** defines what to do with detected portscan traffic. It can be dropped or rejected. When **Log only** is set, traffic will still be allowed but the portscan incident is logged.

✓ Apply

4) SQL Injection

(1-1) admin_login.asp 내용 수정

```

else
    session("user_name") = ""
    session("user_jumin") = ""
    session("id") = ""
    session("name") = ""
    rs("admin_ID") = replace(rs("admin_ID"), "'/'g", "")
    rs("admin_ID") = replace(rs("admin_ID"), "'/'or'/'g", "")
    rs("admin_ID") = replace(rs("admin_ID"), "'/'--/'g", "")
    rs("admin_ID") = replace(rs("admin_ID"), "'/';--/'g", "")
    Session("admin_id") = rs("admin_ID")
    Session("admin_pass") = rs("admin_Pass")
    
```

(1-2) 차단 시도

관리자의 ID와 Password를 입력하세요.

ID

Password

확인

ADODB.Recordset error '800a0cb3'

현재 레코드 집합이 업데이트를 지원하지 않습니다. 이것은 공급자의 제한 또는 선택한 잠금 형식일 수 있습니다.

/admin/admin_login.asp, line 25

5) TCP SYN Flooding, UDP Flooding, ICMP Flooding

(1-1) 레지스트리 편집기 방지하기 위한 값 추가하기



(1-2) 차단 시도1 - 차단 0


```
root@bt:~# hping3 -S -p 23 --flood 10.10.10.20
HPING 10.10.10.20 (eth0 10.10.10.20): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```


```
C:\>netstat -an


Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:80               0.0.0.0:0               LISTENING
TCP    0.0.0.0:135              0.0.0.0:0               LISTENING
TCP    0.0.0.0:445              0.0.0.0:0               LISTENING
TCP    0.0.0.0:1025             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1026             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1028             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1031             0.0.0.0:0               LISTENING
TCP    0.0.0.0:3372             0.0.0.0:0               LISTENING
TCP    10.10.10.20:139          0.0.0.0:0               LISTENING
TCP    10.10.10.20:1433        0.0.0.0:0               LISTENING
TCP    127.0.0.1:1433          0.0.0.0:0               LISTENING
UDP    0.0.0.0:135              *:*:
UDP    0.0.0.0:445              *:*:
UDP    0.0.0.0:1030             *:*:
UDP    0.0.0.0:1434             *:*:
UDP    0.0.0.0:3456             *:*:
UDP    10.10.10.20:137         *:*:
UDP    10.10.10.20:138         *:*:
UDP    10.10.10.20:500         *:*
```


(1-3) 차단 시도2 - 차단0
> ICMP 패킷 확인 불가

| TCP SYN Flood Protection | |
|---|--|
| <input checked="" type="checkbox"/> Use TCP SYN Flood Protection | TCP SYN Flood Protection detects and blocks TCP SYN packet floods. |
| Mode: Source and destination addresses ▼ | |
| Logging: Limited ▼ | |
| Source packet rate (packets/second): 100 | |
| Destination packet rate (packets/second): 200 | |
|  | |

| UDP Flood Protection | |
|---|--|
| <input checked="" type="checkbox"/> Use UDP Flood Protection | UDP Flood Protection detects and blocks UDP packet floods. |
| Mode: Source and destination addresses ▼ | |
| Logging: Limited ▼ | |
| Source packet rate (packets/second): 200 | |
| Destination packet rate (packets/second): 300 | |
|  | |

| ICMP Flood Protection | |
|---|--|
| <input checked="" type="checkbox"/> Use ICMP Flood Protection | ICMP Flood Protection detects and blocks ICMP packet floods. |
| Mode: Source and destination addresses ▼ | |
| Logging: Limited ▼ | |
| Source packet rate (packets/second): 10 | |
| Destination packet rate (packets/second): 20 | |
|  | |

4. 사후처리하기

4-1. 모의해킹 시 탐지나 차단되지 않은 보안위협에 대한 대응 결과를 보고하라.

| 탐지나 차단되지 않은 위협 | 대응 | 결과 |
|------------------|-------------------------------|---------------|
| ARP Spoofing | ARP 테이블 정적 변경 | 차단 0 |
| Bruteforcing | 패스워드 틀린 횟수 제한 | 차단 0 |
| Port Scanning | 포트 닫기 Portscan | 차단 0 |
| XSS | 작성 내용 변경 | 차단 0 |
| SQL Injection | 레지스트리 값 추가 Flood protecton | ICMP만 확인 안 됨. |
| TCP SYN Flooding | | |
| UDP Flooding | | |

4-2. 보완된 정보시스템의 보안설정을 최종 점검하고 취약점 발견 시 추가 대응책을 제시하라.

가상머신 상에서 UTM WebAdmin으로 로그를 확인할 때 ICMP를 확인하지 못한 점과 XSS 공격 시 UTM에서 특정 IP끼리 신호가 가는 것은 확인되었으나 그 로그가 XSS로 인한 로그인지 확인할 수 없다. Sophos community에서도 확인해봤지만 해결할 수 없었다.