
Snort rule 분석

< 공격패킷 생성에 필요한 데이터를 중심으로 >



학교	중앙대학교
이름	송 성 욱

【 Index 】

I. Snort Rule 개념	3
II. Rule 분석	5
1. CC	5
2. DI	7
3. FD	8
4. FS	12
5. LI	16
6. XI	18

Snort Rule 분석

I. snort rule 개념

1. content

○ 기본 사용법

1. content라는 키워드를 작성한다. ex) content
2. 콜론(:)을 붙여 시작을 알린다. ex) content:
3. 따옴표("")로 패턴이 시작됨을 명시한다. ex) content:"
4. 탐지하고자 하는 패턴을 입력한다. ex) content:"pat"
5. 따옴표("")를 한 번 더 붙여 패턴 종결을 명시한다. ex) content:"pat"

○ 옵션

- ! : 입력한 패턴이 매칭되지 않는지 검사
- | : hex값을 표현할 때 사용
- \ : 특수 기호 escape 처리 할 때 사용

○ 사용예

- content:"pattern"; 단순 패턴
- content:"|20|hex|20 28|"; 패턴 + Hex값
- content:"\pattern\"; 사용 불가한 패턴을 escape처리
- content:!\"negate\"; 패킷에 negate 패턴이 없는지 검사

○ content이외의 옵션목록

번호	옵션	설명
1	nocase	대/소문자 구분 하지 않음
2	rawbytes	decode하지 않은 raw data와 매칭 시도
3	depth	payload에서 패턴 매칭을 할 끝 위치 지정
4	offset	payload에서 패턴 매칭을 할 시작 위치 지정
5	distance	이전 content에 매칭된 경우, 패턴 매칭을 시작할 상대 위치 지정
6	within	이전 content에 매칭된 경우, 패턴 매칭을 끝 낼 상대 위치 지정
7	http_client_body	HTTP body 부분에 대해 패턴 매칭 시도
8	http_cookie	HTTP cookie 부분에 대해 패턴 매칭 시도
9	http_raw_cookie	HTTP cookie를 decode하지 않은 부분에 대해 패턴 매칭 시도
10	http_header	HTTP header 부분에 대해 패턴 매칭 시도
11	http_raw_header	HTTP header를 decode하지 않은 부분에 대해 패턴 매칭 시도
12	http_method	HTTP method 부분에 대해 패턴 매칭 시도
13	http_uri	HTTP uri 부분에 대해 패턴 매칭 시도
14	http_raw_uri	HTTP uri를 decode하지 않은 부분에 대해 패턴 매칭 시도
15	http_stat_code	HTTP response 패킷의 stat code 부분에 대해 패턴 매칭 시도
16	http_stat_msg	HTTP response 패킷의 stat msg 부분에 대해 패턴 매칭 시도
17	fast_pattern	longest pattern 지정 - keyword처럼 동작함.

[표 1] 옵션 종류

○ 2장 참고사항

- 16진수 데이터는 |22| 또는 0x22 로 표현하였음.
- Rule이 간단한 경우에는 예시를 한 줄로 표현하였다.
- 실제 http패킷을 단순화 하여 일부만 예시로 표현하였다.

II. Rule 분석

1. CC

- **flow:to_server,established; content:login.php"; nocase; http_uri;**
content:"ACalAuthenticate|3D|inside"; nocase; http_cookie; metadata:service http;
reference:cve

- URI에 "login.php"가 대소문자 구분 없이 포함된다.
 - Cookie헤더에 "ACalAuthenticate|3D|inside"가 대소문자 구분 없이 포함된다.
- ※ 예시) GET /test.com/LOGIn.php ...중략.... Cookie : ACalAuthenticate0x3Dinside

- **flow:to_server,established;**
content:EAAAAPiZE5314QWTlkMUFedwxt0qYWRtaW5pc3RyYXRvcio";
content:"EAAAAPiZE5314QWTlkMUFedwxt0qYWRtaW5pc3RyYXRvcio"; http_cookie;
metadata:service http; reference:cve
 - Cookie헤더에 "EAAAAPiZE5314QWTlkMUFedwxt0qYWRtaW5pc3RyYXRvcio"가 포함된다.
- ※ 예시) GET중략.... Cookie : EAAAAPiZE5314QWTlkMUFedwxt0qYWRtaW5pc3RyYXRvcio

- **flow:to_server,established; content:/get/maincgi.cgi"; fast_pattern:only; http_uri; urilen:16;**
content:"session_id=|22|"; http_cookie; content:"|60|"; within:1000; http_cookie;
pcre:"/session_id=\Wx22[\^Wx22]{0
 - URI길이가 16이고 "/get/maincgi.cgi"를 포함한다.
 - Cookie헤더에 "session_id=|22|"가 포함된다.
 - "session_id=|22|" 뒤에 1000자 이내로 정규표현식 매칭
- ※ 예시)

○ **flow:established, to_server; content:/modTMCM"; fast_pattern:only; http_uri;**
content:"WIFINFOR"; http_cookie; metadata:service http; reference:url

- URI에 "/modTMCM"가 포함된다.

- Cookie헤더에 "WIFINFOR"가 포함된다.

※ 예시) POST /modTMCMCookie : WIFINFOR...

○ **flow:to_server,established; content:C1073"; fast_pattern:only;**
pcre:"/^C1073\w{5}=\w+w*?\w+00/Ci"; metadata:service http; reference:bugtraq

- 패킷 전체에서 "C1073"이 포함된다.

- 정규표현식 매칭

※ 예시)

2. DI

○ **flow:to_server,established; content:|00.jsp"; http_uri; metadata:ruleset community**

- URI에 "|00.jsp"이 포함된다.

※ 예시) GET /test.com/download0x00.jsp (0x00은 16진수 00을 의미)

○ **flow:to_server, established; content:/sap/bc/soap/rfc"; fast_pattern:only; http_uri;**

content:"SOAPAction: urn:sap-com:document:sap:rfc:functions"; http_header;
content:"RZL_READ_DIR_LOCAL"; http_client_body; content:"<FILE_TBL>;
http_client_body; content:"<NAME>"; distance:0; http_client_body; content:"/";
within:100; http_client_body; content:"</NAME>"; within:100; http_client_body;
metadata:policy balanced-ips drop

- URI에 "/sap/bc/soap/rfc"가 포함된다.
- HTTP헤더 전체에서 "SOAPAction: urn:sap-com:document:sap:rfc:functions"가 포함된다.
- HTTP바디에 "RZL_READ_DIR_LOCAL"가 포함된다.
- HTTP바디에 "<FILE_TBL>....<NAME>"가 포함된다. (...은 이곳에 문자가 들어와도 된다는 의미)
- HTTP바디에 "<FILE_TBL>....<NAME>"뒤에 100바이트 이내로 "/"가 포함된다.
- HTTP바디에 "/"뒤에 100바이트 이내로 "</NAME>"가 포함된다.

※ 예시) POST /seculayer/sap/bc/soap/rfc

SOAPAction: urn:sap-com:document:sap:rfc:functions

.....헤더 생략.....

.....바디 시작.....

RZL_READ_DIR_LOCAL...<FILE_TBL>...<NAME>...../.....</NAME>

○ **flow:to_server,established; content:/rpc/dir"; fast_pattern:only; http_uri; content:"path=";**

nocase; http_uri; metadata:ruleset community

- URI에 "/rpc/dir"이 포함된다.
- URI에 "path="이 대소문자구분없이 포함된다.

※ 예시) GET /test.com/rpc/dir/getid?path=1234 ...

3. FD

- **flow:to_server,established; content:csp."; http_uri; metadata:ruleset community**
 - URI에 ".csp."이 포함된다.

※ 예시) GET /test.com/download.csp.
- **flow:to_server,established; content:pl"; http_uri; content:".pl"; content:"."; within:1; metadata:ruleset community**
 - URI에 ".pl"이 포함된다.
 - HTTP바디에 ".pl."이 포함된다.

※ 예시) GET /test.com/download.pl getfile=download.pl.
- **flow:to_server,established; content:exe"; http_uri; content:".exe"; content:"."; within:1; metadata:ruleset community**
 - URI에 ".exe"이 포함된다.
 - HTTP바디에 ".exe."이 포함된다.

※ 예시) GET /test.com/download.exe getfile=download.exe.
- **flow:to_server,established; content:header.php"; fast_pattern:only; http_uri; content:"Vb8878b936c2bd8ae0cab="; nocase; pcre:"/Vb8878b936c2bd8ae0cab=(https?|ftps?)i"; metadata:service http; reference:bugtraq**
 - URI에 "header.php"이 포함된다.
 - HTTP패킷 전체에서 "Vb8878b936c2bd8ae0cab="이 대소문자 구분없이 포함된다.
 - 정규표현식 매칭

※ 예시)

○ flow:to_server,established; content:<NAME>SRS</NAME>"; nocase; http_client_body;
content:"<OPERATION>4</OPERATION>"; nocase; http_client_body;
content:"<CMD>103</CMD>"; fast_pattern:only; http_client_body;
content:"<PATH>c:|5C|"; nocase; http_client_body; metadata:service http;
reference:bugtraq

- HTTP바디에 "<NAME>SRS</NAME>"이 대소문자 구분 없이 포함된다.
- HTTP바디에 "<CMD>103</CMD>"이 포함된다.
- HTTP바디에 "<PATH>c:|5C|"이 대소문자 구분 없이 포함된다.

※ 예시) GET /test/dir1/a.php

...바디 시작....

<NAME>SRS</NAME>....<CMD>103</CMD>...<PATH>c:0x5C...

○ flow:to_server,established; content:/limesurvey/index.php/admin/update(sa/backup";
fast_pattern:only; http_uri; content:"datasupdateinfo="; nocase; http_client_body;
pcre:"/(^|&)datasupdateinfo=[^&]*?(Wx2e|%2e){2}(Wx2fWx5c)|%2f|%5c)/Pim";
metadata:service http; reference:url

- URI에 "/limesurvey/index.php/admin/update(sa/backup"이 포함된다.
- HTTP바디에 "datasupdateinfo="이 포함된다.
- 정규표현식 매칭

※ 예시)

○ flow:to_server,established; content:/pls/"; http_uri;
content:"/ADI_display_report.DisplayFile?"; fast_pattern:only; http_uri;
content:"P_DOCID="; http_uri; metadata:service http; reference:bugtraq

- URI에 "/pls/"이 포함된다.
- URI에 "/ADI_display_report.DisplayFile?"이 포함된다.
- URI에 "P_DOCID="이 포함된다.

※ 예시) GET /pls/ADI_display_report.DisplayFile?P_DOCID=

- **flow:to_server,established; content:/html/en/confAccessProt.html"; fast_pattern:only; http_uri; metadata:policy max-detect-ips dro**
 - URI에 "/html/en/confAccessProt.html"이 포함된다.

※ 예시) GET html/en/confAccessProt.html
- **flow:to_server,established; content:download.conf"; fast_pattern:only; http_uri; content:"filename="; nocase; http_uri; metadata:ruleset community**
 - URI에 "download.conf"이 포함된다.
 - URI에 "filename="이 대소문자 구분 없이 포함된다.

※ 예시) GET /shopping/category1/download.conf?filename=123.txt
- **flow:to_server,established; content:/goform/down_cfg_file"; fast_pattern:only; http_uri; urilen:21; metadata:policy max-detect-ips drop**
 - URI길이는 21이고 "/goform/down_cfg_file"이 포함된다.

※ 예시) GET /goform/down_cfg_file ...
- **flow:to_server,established;**
content:/DesktopModules/DreamSlider/DownloadProvider.aspx"; fast_pattern:only; nocase; http_uri; content:"file="; nocase; http_uri; metadata:ruleset community
 - URI에 "/DesktopModules/DreamSlider/DownloadProvider.aspx"이 대소문자 구분 없이 포함된다.
 - URI에 "file="이 대소문자 구분 없이 포함된다.

※ 예시) GET /DesktopModules/DreamSlider/DownloadProvider.aspx?file=passwd ...

- flow:to_server,established; content:ApplicationDetails.aspx"; fast_pattern:only;
content:"__VIEWSTATE"; nocase; content:"__EVENTVALIDATION"; nocase;
content:"Port+Selection"; nocase; content:"portTextBox"; nocase;
content:"nameTextBox"; nocase; content:"descriptionTextBox"; nocase;
content:"appIdTextBox"; nocase; content:"clrVersionDropDownList"; nocase;
content:"submitImageButton.x"; nocase; content:"submitImageButton.y"; nocase;
content:"physicalPathTextBox"; nocase; content:"defaultDocumentTextBox"; nocase;
metadata:service http; reference:url
 - HTTP패킷 전체에서 "ApplicationDetails.aspx"가 포함된다.
 - HTTP패킷 전체에서 "__VIEWSTATE"가 대소문자 구분없이 포함된다.
 - HTTP패킷 전체에서 "__EVENTVALIDATION"가 대소문자 구분없이 포함된다.
 - HTTP패킷 전체에서 "Port+Selection"가 대소문자 구분없이 포함된다.
 - HTTP패킷 전체에서 "portTextBox"가 대소문자 구분없이 포함된다.
 - HTTP패킷 전체에서 "nameTextBox"가 대소문자 구분없이 포함된다.
 - HTTP패킷 전체에서 "descriptionTextBox"가 대소문자 구분없이 포함된다.
 - HTTP패킷 전체에서 "appIdTextBox"가 대소문자 구분없이 포함된다.
 - HTTP패킷 전체에서 "clrVersionDropDownList"가 대소문자 구분없이 포함된다.
 - HTTP패킷 전체에서 "submitButton.x"가 대소문자 구분없이 포함된다.
 - HTTP패킷 전체에서 "submitButton.y"가 대소문자 구분없이 포함된다.
 - HTTP패킷 전체에서 "physicalPathTextBox"가 대소문자 구분없이 포함된다.
 - HTTP패킷 전체에서 "defaultDocumentTextBox"가 대소문자 구분없이 포함된다.

※ 예시) GET /test/download/

...바디시작...

ApplicationDetails.aspx...__VIEWSTATE...__EVENTVALIDATION...
Port+Selection...portTextBox...nameTextBox...descriptionTextBox...appIdTextBox...
clrVersionDropDownList...submitButton.x...submitButton.y...
physicalPathTextBox...defaultDocumentTextBox

4. FS

- `flow:to_server,established; content:/content/"; fast_pattern:only;`
`pcre:"/\W/content\W/[^\W\Wn\Wx20]*\Wx2emp3/smi"; metadata:policy max-detect-ips drop`
 - HTTP패킷 전체에서 "/content/"이 포함된다.
 - 정규표현식 매칭

※ 예시)

- `flow:to_server,established; content:GET "; depth:4; nocase; content:"evtdump?";`
`distance:0; nocase; pcre:"/evtdump\Wx3f.*?\Wx2525[^Wx20]*?\Wx20HTTP/i";`
`metadata:policy max-detect-ips drop`
 - HTTP패킷 처음 4바이트가 "GET "이다.
 - "GET "뒤에 "evtdump?"가 대소문자 구분 없이 포함된다.
 - 정규표현식 매칭

※ 예시)

- `flow:to_server,established; content:application/x-www-form-urlencoded"; http_header;`
`content:"abc=%25s%25s"; fast_pattern; metadata:policy max-detect-ips drop`
 - HTTP헤더에 "application/x-www-form-urlencoded"이 포함된다.
 - HTTP패킷 전체에서 "abc=%25s%25s""가 포함된다.

※ 예시) POST /test/admin

Content-type : application/x-www-form-urlencoded
....헤더 중략...
....바디 시작...
abc=%25s%25s&ccc=123...

○ **flow:to_server,established; content:PROPFIND"; depth:8; fast_pattern; nocase; content:"<?xml"; content:"encoding"; within:30; pcre:"/W<W?xml[^W>]+encodingWs*W=Ws*(W|W")[^WW" W>W%]*W%/"; metadata:service http; reference:bugtraq**

- HTTP패킷 처음 8바이트가 "PROPFIND"이다 (대소문자 구분X).
- HTTP패킷 전체에서 "<?xml"가 포함된다.
- "<?xml"뒤에 30바이트 내로 "encoding"이 들어간다.
- 정규표현식 매칭

※ 예시) PROPFIND /test/admin

```
Content-type : application/x-www-form-urlencoded
....헤더 중략...
....바디 시작...
<?xml .... encoding ...
```

○ **flow:to_server,established; content:LOCK"; nocase; http_method; content:"<?xml"; fast_pattern; content:"encoding"; within:50; pcre:"/W<W?xml[^W>]+encodingWs*W=Ws*(W|W")[^WW" W>W%]*W%/"; metadata:service http; reference:bugtraq**

- HTTP메소드가 "LOCK"이다. (대소문자 구분X)
- HTTP패킷 전체에서 "<?xml"가 포함된다.
- "<?xml"뒤에 50바이트 내로 "encoding"이 들어간다.
- 정규표현식 매칭

※ 예시) LOCK /test/admin

```
Content-type : application/x-www-form-urlencoded
....헤더 중략...
....바디 시작...
<?xml .... encoding ...
```

- `flow:to_server,established; content:Connection|3A|"; nocase; http_raw_header; content:"%"; distance:0; http_raw_header; pcre:"^ConnectionWx3A[^WrWn]+%/smiD"; metadata:service http; reference:bugtraq`
 - HTTP헤더에 "Connection|3A|"이 포함된다. (Decode하지 않은 헤더)
 - "Connection|3A|" 바로 뒤에 "%"이 포함된다.
 - 정규표현식 매칭

※ 예시)
- `flow:to_server,established; content:/OvCgi/nnmRptConfig.exe"; fast_pattern:only; http_uri; content:"Action=Create"; nocase; pcre:"TemplateWx3D[^Wx26]*?Wx25Wd*[xsdn]/i"; metadata:policy max-detect-ips drop`
 - URI에 "/OvCgi/nnmRptConfig.exe"이 포함된다.
 - HTTP패킷 전체에서 "Action=Create"이 대소문자 구분없이 포함된다.
 - 정규표현식 매칭

※ 예시)
- `flow:to_server,established; content:%25hn"; fast_pattern:only; http_uri; pcre:"/(%(\Wd+\Wx24)?(\Wd+)?[nxcsd])\{3\}/Ui"; metadata:service http; reference:cve`
 - URI에 "%25hn"이 포함된다.
 - 정규표현식 매칭

※ 예시) GET /test/upload.php?=%25hn%25hn ...
- `flow:to_server,established; content:/cgi-sys/cgiecho/~"; fast_pattern:only; http_uri; content:"failure=stdin"; nocase; http_uri; content:"%p"; http_client_body; content:"%p"; within:10; http_client_body; content:"%p"; within:10; http_client_body; content:"%p"; within:10; http_client_body; metadata:policy max-detect-ips drop`
 - URI에 "/cgi-sys/cgiecho/~"이 포함된다.
 - URI에 "failure=stdin"이 대소문자 구분 없이 포함된다.
 - HTTP바디에 "%p"가 4개 이상 포함된다. "%p"들은 서로 10바이트 이내에 위치한다.

※ 예시) POST /cgi-sys/cgiecho/~/test?failure=stdin

Content-type : application/x-www-form-urlencoded

....헤더 중략...

....바디 시작...

abc=%p...%p...%p...%p...&upload=a.txt

- **flow:to_server,established; content:/hello/~/"; fast_pattern:only; http_uri;**
content:"failure=stdin"; nocase; http_uri; content:"%p"; http_client_body;
content:"%p"; within:10; http_client_body; content:"%p"; within:10; http_client_body;
content:"%p"; within:10; http_client_body; metadata:policy max-detect-ips drop

- URI에 "/hello/~/"이 포함된다.
- URI에 "failure=stdin"이 대소문자 구분 없이 포함된다.
- HTTP바디에 "%p"가 4개 이상 포함된다. "%p"들은 서로 10바이트 이내에 위치한다.

※ 예시) POST /test/admin/hello/~/test?failure=stdin

Content-type : application/x-www-form-urlencoded

....헤더 중략...

....바디 시작...

abc=%p...%p...%p...%p...&upload=a.txt

5. LI

○ **flow:to_server,established; content:/component/users/"; fast_pattern; http_uri;**
content:"task=user.login"; within:25; http_uri; content:"username="; nocase; http_uri;
pcre:"/[?&]username=[^&]*?(Wx28Wx29Wx7C!<=>Wx2A])/Ui"; metadata:policy
max-detect-ips drop

- URI에 "/component/users/"이 포함된다.
- "/component/users/"뒤에 25바이트 이내로 "task=user.login"이 들어간다.
- URI에 "username="이 대소문자 구분 없이 포함된다.
- 정규표현식 매칭

※ 예시)

○ **flow:to_server,established; content:/component/users/"; fast_pattern; http_uri;**
content:"task=user.login"; within:25; http_uri; content:"username="; nocase;
http_client_body;
pcre:"/(^|&)username=[^&]*?(Wx28Wx29Wx7C!<=>Wx2A]|%(28|29|7C|21|3C|3D|3E|2A))/Pi
m"; metadata:policy max-detect-ips drop

- URI에 "/component/users/"이 포함된다.
- "/component/users/"뒤에 25바이트 이내로 "task=user.login"이 들어간다.
- HTTP바디에 "username="이 대소문자 구분 없이 포함된다.
- 정규표현식 매칭

※ 예시)

○ flow:to_server,established; content:/component/users/"; fast_pattern; http_uri;
content:"task=user.login"; within:25; http_uri; content:"username="; nocase;
http_client_body; content:"Content-Disposition"; nocase; http_client_body;
pcre:"/username((?!^--).)*?[WrWn]{2

- URI에 "/component/users/"이 포함된다.
- "/component/users/" 뒤에 25바이트 이내로 "task=user.login"이 들어간다.
- HTTP바디에 "username="이 대소문자 구분 없이 포함된다.
- HTTP바디에 "Content-Disposition"이 대소문자 구분 없이 포함된다.
- 정규표현식 매칭

※ 예시)

6. XI

- **flow:established,to_server; content:[27]) and string"; fast_pattern:only; http_uri; content:"USER-AGENT|3A| Python"; http_header; metadata:service http; reference:url**
 - URI에 "|27) and string"이 포함된다.
 - HTTP헤더에 "USER-AGENT|3A| Python"이 포함된다.

※ 예시) GET /test/admin/download.php?fname=0x27) and string
USER-AGENT: Python

- **flow:established,to_server; content:[27]) and count(("; fast_pattern:only; http_uri; content:"USER-AGENT|3A| Python"; http_header; metadata:service http; reference:url**
 - URI에 "|27) and count(("이 포함된다.
 - HTTP헤더에 "USER-AGENT|3A| Python"이 포함된다.

※ 예시) GET /test/admin/download.php?fname=0x27 and count()
USER-AGENT: Python

- **flow:established,to_server; content:[27]) and doc((document-uri(/)))=(/); fast_pattern:only; http_uri; content:"USER-AGENT|3A| Python"; http_header; metadata:service http; reference:url**
 - URI에 "|27) and doc((document-uri(/)))=(/"이 포함된다.
 - HTTP헤더에 "USER-AGENT|3A| Python"이 포함된다.

※ 예시) GET /test/admin/download.php?fname=0x27) and doc((document-uri(/)))=(/
USER-AGENT: Python