DAFTAR PUSTAKA

Agustian, Hari. (2020). Implementasi Keamanan Wireless LAN Menggunakan Snort dan IPTables. Universitas Dehasen Bengkulu.

Bangga, I Gede Walid. (2022). Simulasi Snort Sebagai Alat Pendeteksi Intrusi Pada Web DAMN Vulnerable Web Application. Jurnal Rekayasa Informasi.

Banjo, Chika Yinka. (2022). Intrusion Detection Using Anomaly Detection Algorithm and Snort. LNDECT Vol 109.

Dar, Muhammad Halmi. (2018). Implementasi Snort Intrusion Detection System Pada Sistem Jaringan Komputer. Jurnal Rekayasa Informasi. Jurnal ULB.

Dasmen, Rahmat Novrianda. (2022). Penerapan Snort Sebagai Sistem PendeteksiSerangan Keamanan Jaringan. Universitas Bina Darma.

Erlansari, Aan. (2020). Early Intrusion Detection System (IDS) Using Snort And Telegram Approach. SISFORMA.

Fachri, Barani. (2020). Simulasi Penggunaan *Intrusion Detection System* (IDS) Sebagai Kemanan Jaringan dan Komputer. STMIK Budidarma.

Fauzi, Raihan. (2023). Sistem Keamanan Jaringan Komputer Berbasis Teknik *Intrusion Detection System* (IDS) Untuk Mendeteksi Serangan *Distributed Denial of Service* (DDOS). Repository Tunas Bangsa.

Gupta, Alka. (2020). Performance Analysis and Comparison of Snort on Various Platform. International Journal of Computer Information Syste and Industrial Management Applications.

Jain, G. (2021). Application of Snort and Wireshark in Network Traffic Analysis. IOP Publishing Ltd.

Kunhare, Nilesh. (2020). Network Packet Analysis in Real Time Traffic and Study of Snort IDS During the Variants of DoS Attacks. AISC Vol 1179.

bin. (2019). Implementasi *Network Intrusion Detection System* (NIDS) am Sitem Keamanan *Open Cloud Computing*. Akademi Maritim gyakarta.

Purba, Winrou Wesley. (2021). Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan Snort. Satya Wacana Christian University.

Ramadhan, Idrus. (2019). Keamanan Jaringan Dengan Snort IDS Menggunakan Metode Forensic Jaringan. Jurnal Ilmiah MIKA AMIK Al Muslim.

Razak, Shukor. (2021). Anomaly *Base*d Intrusion Detection System in IoT UsingDeep Learning: A Systematic Literature Review. IEEE.

Santoso, Joko Dwi. (2019). Keamanan Jaringan Nirkabel Menggunakan WirelessIntrusion Detection System**.** INFOS Journal.

Sharma, Shubham. (2022). Intrusion Detection and Prevention System Using Snort. LNDECT Vol 86.

Stephani, Elsa. (2020). Implementasi dan Analisa Keamanan Jaringan IDS (*Intrusion Detection System*). Jurnal ITSI.

Triandini, Rizki. (2020). Implementasi Intrusion Detection System Menggunakan Banyard dan *Base* Pada Sistem Operasi Linux. Repository Unikom.

Usama, Usama. (2019). Analisis Kinerja Sitem Pencegahan Penyusupan JaringanMenggunkan Honeypot Pada Windows. Repository ITN Malang.

Wang, Shaoqian. (2020). Intrusion Detection System for WiFi Network: A Deep Learning Approach. IEEE.

LAMPIRAN

Lampiran 1

Konfigurasi rules yang digunakan pada Snort

C: > Snort > etc > snort.conf

```
# Setup the network addresses you are protecting
Ipvar HOME_NET 192.168.1.9
# Setup the external network addresses. Leave as “any” in most situations
Ipvar EXTERNAL_NET !$HOME_NET
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH
/etc/snort/preproc_rules
var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists
config daq: afpacket
config daq_dir: /usr/local/lib/snort_dynamicrules
config daq_mode: inline
config policy_mode: inline
config daq_var: queue=0
# path to dyanmic preprocessor libraries
dynamicpreprocessor dictory c:\snort\lib\snort_dynamicpreprocessor
# path to base preprocessor engine
dynamicengine c:\snort\lib\snort_dynamicengine\sf.engine.dll
# path to dynamic rules libraries
# dynamicdetection directory
/usr/local/lib/snort_dynamicrles

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.1.9

# FTP / Telnet normalization and anomaly detection.  For more information, see README.ftptelnet
preprocessor ftp_telnet: global inspection_type stateful encrypted_traffic no check_encrypted
preprocessor ftp_telnet_protocol: telnet \
    ayt_attack_thresh 20 \
    normalize ports { 23 } \
    detect_anomalies
```

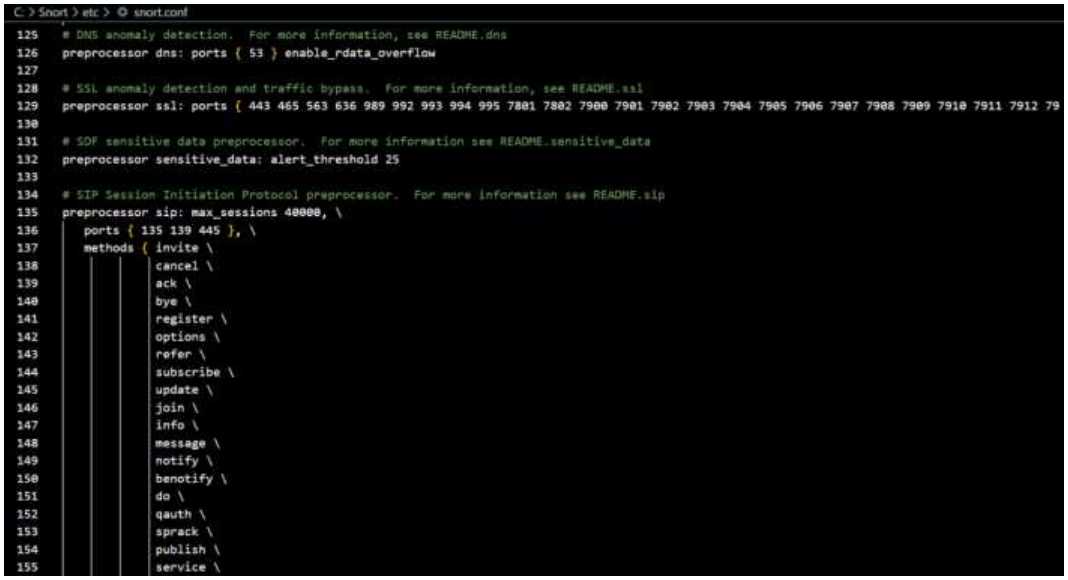
```
preprocessor ftp_telnet_protocol: ftp server default \
    def_max_param_len 100 \
    ports { 21 2100 3535 } \
    telnet_cmds yes \
    ignore_telnet_erase_cmds yes \
    ftp_cmds { ABOR ACCT ADAT ALLO APPE AUTH CCC CDUP } \
    ftp_cmds { CEL CLNT CMD CONF CWD DELE ENC EPRT } \
    ftp_cmds { EPSV ESTA ESTP FEAT HELP LANG LIST LPRT } \
    ftp_cmds { LPSV MACB MAIL MDTM MIC MKD MLSD MLST } \
    ftp_cmds { MODE NLST NOOP OPTS PASS PASV PBSZ PORT } \
    ftp_cmds { PROT PWD QUIT REIN REST RETR RMD RNFR } \
    ftp_cmds { RNTO SDUP SITE SIZE SMNT STAT STOR STOU } \
    ftp_cmds { STRU SYST TEST TYPE USER XCUP XCRC XCWD } \
    ftp_cmds { XMAS XMD5 XMKD XPWD XRCP XRMD XRSQ XSEM } \
    ftp_cmds { XSEN XSHA1 XSHA256 } \
    alt_max_param_len 0 { ABOR CCC CDUP ESTA FEAT LPSV NOOP PASV PWD QUIT REIN STOU SYST XCUP XPWD } \
    alt_max_param_len 200 { ALLO APPE CMD HELP NLST RETR RNFR STOR STOU XMKD } \
    alt_max_param_len 256 { CWD RNTO } \
    alt_max_param_len 400 { PORT } \
    alt_max_param_len 512 { SIZE } \
    chk_str_fmt { ACCT ADAT ALLO APPE AUTH CEL CLNT CMD } \
    chk_str_fmt { CONF CWD DELE ENC EPRT EPSV ESTP HELP } \
    chk_str_fmt { LANG LIST LPRT MACB MAIL MDTM MIC MKD } \
    chk_str_fmt { MLSD MLST MODE NLST OPTS PASS PBSZ PORT } \
    chk_str_fmt { PROT REST RETR RMD RNFR RNTO SDUP SITE } \
    chk_str_fmt { SIZE SMNT STAT STOR STRU TEST TYPE USER } \
    chk_str_fmt { XCRC XCWD XMAS XMD5 XMKD XRCP XRMD XRSQ } \
    chk_str_fmt { XSEM XSEN XSHA1 XSHA256 } \
    cmd_validity ALLO < int [ char R int ] > \
    cmd_validity EPSV < [ { char 12 | char A char L char L } ] > \
    cmd_validity MACB < string > \
```

C: > Snort > etc > snort.conf

```
64      cmd_validity MDTM < [ date nnnnnnnnnnnnnn[.n[n[n]]] ] string > \
65      cmd_validity MODE < char ASBCZ > \
66      cmd_validity PORT < host_port > \
67      cmd_validity PROT < char CSEP > \
68      cmd_validity STRU < char FRPO [ string ] > \
69      cmd_validity TYPE < { char AE [ char NTC ] | char I | char L [ number ] } >
70    preprocessor ftp_telnet_protocol: ftp client default \
71      max_resp_len 256 \
72      bounce yes \
73      ignore_telnet_erase_cmds yes \
74      telnet_cmds yes
75
76
77    # SMTP normalization and anomaly detection.  For more information, see README.SMTP
78    preprocessor smtp: ports { 25 465 587 691 } \
79      inspection_type stateful \
80      b64_decode_depth 0 \
81      qp_decode_depth 0 \
82      bitenc_decode_depth 0 \
83      uu_decode_depth 0 \
84      log_mailfrom \
85      log_rcptto \
86      log_filename \
87      log_email_hdrs \
88      normalize cmds \
89      normalize_cmds { ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY } \
90      normalize_cmds { EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML } \
91      normalize_cmds { STARTTLS TICK TIME TURN TURNME VERB VRFY X-ADAT X-DRCP X-ERCP X-EXCH50 } \
92      normalize_cmds { X-EXPS X-LINK2STATE XADR XAUTH XCIR XEXCH50 XGEN XLICENSE XQUE XSTA XTRN XUSR } \
93      max_command_line_len 512 \
94      max_header_line_len 1000 \
```

C: > Snort > etc > snort.conf

```
95      max_response_line_len 512 \
96      alt_max_command_line_len 260 { MAIL } \
97      alt_max_command_line_len 300 { RCPT } \
98      alt_max_command_line_len 500 { HELP HELO ETRN EHLO } \
99      alt_max_command_line_len 255 { EXPN VRFY ATRN SIZE BDAT DEBUG EMAL ESAM ESND ESOM EVFY IDENT NOOP RSET } \
100     alt_max_command_line_len 246 { SEND SAML SOML AUTH TURN ETRN DATA RSET QUIT ONEX QUEU STARTTLS TICK TIME TURNME VERB X-EXPS X-LINK2STAT
101     valid_cmds { ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY } \
102     valid_cmds { EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML } \
103     valid_cmds { STARTTLS TICK TIME TURN TURNME VERB VRFY X-ADAT X-DRCP X-ERCP X-EXCH50 } \
104     valid_cmds { X-EXPS X-LINK2STATE XADR XAUTH XCIR XEXCH50 XGEN XLICENSE XQUE XSTA XTRN XUSR } \
105     xlink2state { enabled }
106
107
108
109   # SSH anomaly detection.  For more information, see README.ssh
110   preprocessor ssh: server_ports { 22 } \
111                     autodetect \
112                     max_client_bytes 65500 \
113                     max_encrypted_packets 20 \
114                     max_server_version_len 100 \
115                     enable_respoverflow enable_ssh1crc32 \
116                     enable_srvoverflow enable_protomismatch
117
118   # SMB / DCE-RPC normalization and anomaly detection.  For more information, see README.dcerpc2
119   preprocessor dcerpc2: memcap 102400, events [co ]
120   preprocessor dcerpc2_server: default, policy WinXP, \
121     detect [smb [139,445], tcp 135, udp 135, rpc-over-http-server 593], \
122     autodetect [tcp 1025:, udp 1025:, rpc-over-http-server 1025:], \
123     smb_max_chain 3, smb_invalid_shares ["C$", "D$", "ADMIN$"]
124
```



```
C: > Snort > etc > ⚙ snort.conf
125  # DNS anomaly detection.  For more information, see README.dns
126  preprocessor dns: ports { 53 } enable_rdata_overflow
127
128  # SSL anomaly detection and traffic bypass.  For more information, see README.ssl
129  preprocessor ssl: ports { 443 465 563 636 989 992 993 994 995 7801 7802 7900 7901 7902 7903 7904 7905 7906 7907 7908 7909 7910 7911 7912 79
130
131  # SDF sensitive data preprocessor.  For more information see README.sensitive_data
132  preprocessor sensitive_data: alert_threshold 25
133
134  # SIP Session Initiation Protocol preprocessor.  For more information see README.sip
135  preprocessor sip: max_sessions 40000, \
136    ports { 135 139 445 }, \
137    methods { invite \
138              cancel \
139              ack \
140              bye \
141              register \
142              options \
143              refer \
144              subscribe \
145              update \
146              join \
147              info \
148              message \
149              notify \
150              benotify \
151              do \
152              qauth \
153              sprack \
154              publish \
155              service \
```

C: > Snort > etc > ⚙ snort.conf

```
155              service \
156              unsubscribe \
157              prack }, \
158      max_uri_len 512, \
159      max_call_id_len 80, \
160      max_requestName_len 20, \
161      max_from_len 256, \
162      max_to_len 256, \
163      max_via_len 1024, \
164      max_contact_len 512, \
165      max_content_len 2048
166
167  # IMAP preprocessor.  For more information see README.imap
168  preprocessor imap: \
169      ports { 143 } \
170      b64_decode_depth 0 \
171      qp_decode_depth 0 \
172      bitenc_decode_depth 0 \
173      uu_decode_depth 0
174
175  # POP preprocessor. For more information see README.pop
176  preprocessor pop: \
177      ports { 110 } \
178      b64_decode_depth 0 \
179      qp_decode_depth 0 \
180      bitenc_decode_depth 0 \
181      uu_decode_depth 0
182
183  # Modbus preprocessor. For more information see README.modbus
184  preprocessor modbus: ports { 502 }
185
```

C: > Snort > etc > snort.conf

```
186   # DNP3 preprocessor. For more information see README.dnp3
187   preprocessor dnp3: ports { 20000 } \
188       memcap 262144 \
189       check_crc
190
191   # Reputation preprocessor. For more information see README.reputatic
192   preprocessor reputation: \
193       memcap 500, \
194       priority whitelist, \
195       nested_ip inner#, \
196
197   # metadata reference data.  do not modify these lines
198   include classification.config
199   include reference.config
200
201   include c:\snort\etc\classification.config
202   include c:\snort\etc\reference.config
203
204   # site specific rules
205   include c:\snort\rules\snort3-community.rules
206   include c:\snort\rules\local.rules
207
208   include $RULE_PATH/app-detect.rules
209   include $RULE_PATH/attack-responses.rules
210   include $RULE_PATH/backdoor.rules
211   include $RULE_PATH/bad-traffic.rules
212   include $RULE_PATH/blacklist.rules
213   include $RULE_PATH/botnet-cnc.rules
214   include $RULE_PATH/browser-chrome.rules
215   include $RULE_PATH/browser-firefox.rules
216   include $RULE_PATH/browser-ie.rules
217   include $RULE_PATH/browser-other.rules
```

C: > Snort > etc > snort.conf

```
include $RULE_PATH/browser-other.rules
include $RULE_PATH/browser-plugins.rules
include $RULE_PATH/browser-webkit.rules
include $RULE_PATH/chat.rules
include $RULE_PATH/content-replace.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/experimental.rules
include $RULE_PATH/exploit-kit.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/file-executable.rules
include $RULE_PATH/file-flash.rules
include $RULE_PATH/file-identify.rules
include $RULE_PATH/file-image.rules
include $RULE_PATH/file-multimedia.rules
include $RULE_PATH/file-office.rules
include $RULE_PATH/file-other.rules
include $RULE_PATH/file-pdf.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/icmp-info.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/imap.rules
include $RULE_PATH/indicator-compromise.rules
include $RULE_PATH/indicator-obfuscation.rules
include $RULE_PATH/indicator-shellcode.rules
include $RULE_PATH/info.rules
include $RULE_PATH/malware-backdoor.rules
include $RULE_PATH/malware-cnc.rules
include $RULE_PATH/malware-other.rules
include $RULE_PATH/malware-tools.rules
```

C: > Snort > etc > snort.conf

```
249    include $RULE_PATH/misc.rules
250    include $RULE_PATH/multimedia.rules
251    include $RULE_PATH/mysql.rules
252    include $RULE_PATH/netbios.rules
253    include $RULE_PATH/nntp.rules
254    include $RULE_PATH/oracle.rules
255    include $RULE_PATH/os-linux.rules
256    include $RULE_PATH/os-other.rules
257    include $RULE_PATH/os-solaris.rules
258    include $RULE_PATH/os-windows.rules
259    include $RULE_PATH/other-ids.rules
260    include $RULE_PATH/p2p.rules
261    include $RULE_PATH/phishing-spam.rules
262    include $RULE_PATH/policy-multimedia.rules
263    include $RULE_PATH/policy-other.rules
264    include $RULE_PATH/policy.rules
265    include $RULE_PATH/policy-social.rules
266    include $RULE_PATH/policy-spam.rules
267    include $RULE_PATH/pop2.rules
268    include $RULE_PATH/pop3.rules
269    include $RULE_PATH/protocol-finger.rules
270    include $RULE_PATH/protocol-ftp.rules
271    include $RULE_PATH/protocol-icmp.rules
272    include $RULE_PATH/protocol-imap.rules
273    include $RULE_PATH/protocol-pop.rules
274    include $RULE_PATH/protocol-services.rules
275    include $RULE_PATH/protocol-voip.rules
276    include $RULE_PATH/pua-adware.rules
277    include $RULE_PATH/pua-other.rules
278    include $RULE_PATH/pua-p2p.rules
279    include $RULE_PATH/pua-toolbars.rules
```

C: > Snort > etc > snort.conf

```
include $RULE_PATH/rpc.rules
include $RULE_PATH/rservices.rules
include $RULE_PATH/scada.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/server-apache.rules
include $RULE_PATH/server-iis.rules
include $RULE_PATH/server-mail.rules
include $RULE_PATH/server-mssql.rules
include $RULE_PATH/server-mysql.rules
include $RULE_PATH/server-oracle.rules
include $RULE_PATH/server-other.rules
include $RULE_PATH/server-webapp.rules
include $RULE_PATH/shellcode.rules
include $RULE_PATH/smtp.rules
include $RULE_PATH/snmp.rules
include $RULE_PATH/specific-threats.rules
include $RULE_PATH/spyware-put.rules
include $RULE_PATH/sql.rules
include $RULE_PATH/telnet.rules
include $RULE_PATH/tftp.rules
include $RULE_PATH/virus.rules
include $RULE_PATH/voip.rules
include $RULE_PATH/web-activex.rules
include $RULE_PATH/web-attacks.rules
include $RULE_PATH/web-cgi.rules
include $RULE_PATH/web-client.rules
include $RULE_PATH/web-coldfusion.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-php.rules
```

C: > Snort > rules > local.rules

```
#LOCAL RULES


alert icmp any any -> any any (msg:"PING OF DEATH"; fragoffset:0; fragbits:65500; content:"abcdefgh"; depth:8; sid:100001;)
alert icmp any any -> any any (msg:"PING FLOOD"; icode:0; itype:8; threshold: type both, track by_src, count 10, seconds 60; sid:100002;)
alert tcp any any -> any any (msg:"PORT SCANNING"; flags:S; threshold: type both, track by_src, count 3, seconds 60; sid:100003;)


```