

Nama : kholil anggara
Nim : 090111320031

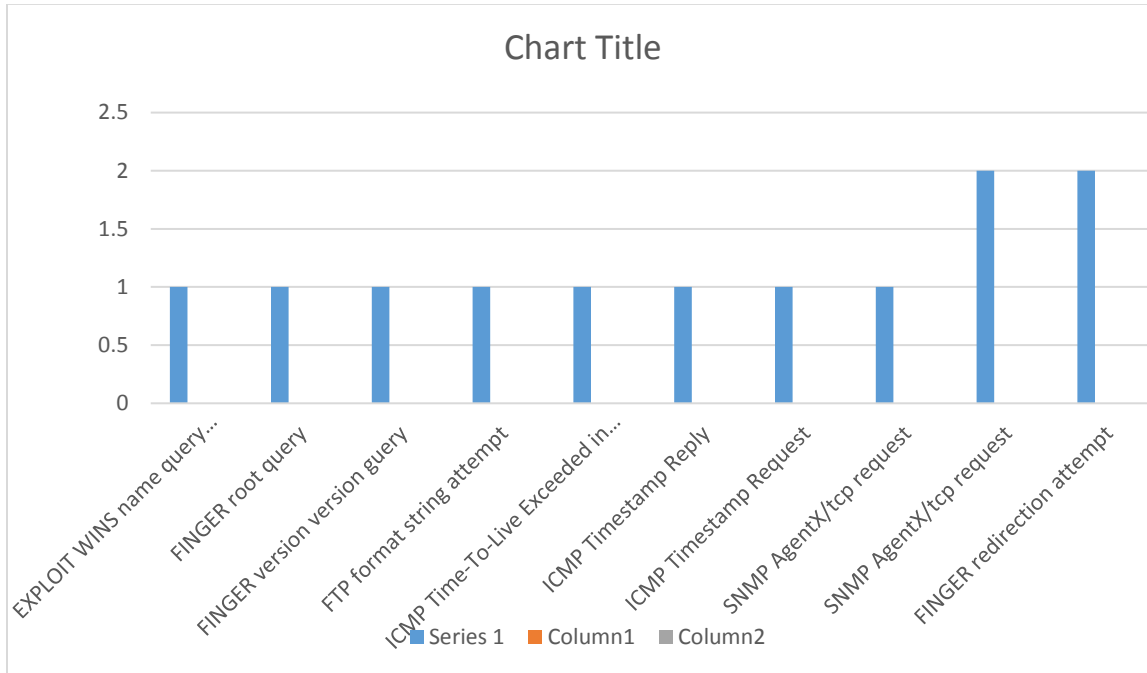
IDS menggunakan SNORT

jumlah	Alert
1	EXPLOIT WINS name query overflow attempt TCP
1	FINGER root query
1	FINGER version version guery
1	FTP format string attempt
1	ICMP PING NMAP
1	ICMP Time-To-Live Exceeded in Transit
1	ICMP Timestamp Reply
1	ICMP Timestamp Request
1	SNMP AgentX/tcp request
2	SNMP AgentX/tcp request
2	FINGER redirection attempt
2	FINGER remote command execution attempt
2	FTP command overflow attempt
2	alert ICMP Destination Unreachable Port Unreachable
2	alert ICMP Destination Unreachable Port Unreachable
2	ICMP PING undefined code
2	WEB-MISC robots.txt access
3	FINGER . query
3	ICMP Echo Reply
3	ICMP PING A21
4	FINGER 0 query
8	SCAN nmap XMAS
9	FINGER null request
12	ICMP Destination Unreachable Communication Administratively Prohibited
12	SCAN UPnP service discover attempt
13	MISC UPnP malformed advertisement
75	SNMP request tcp

Ada 75 jenis alert yang ditemukan pada website detik.com , contohnya dapat dilihat pada table diatas.

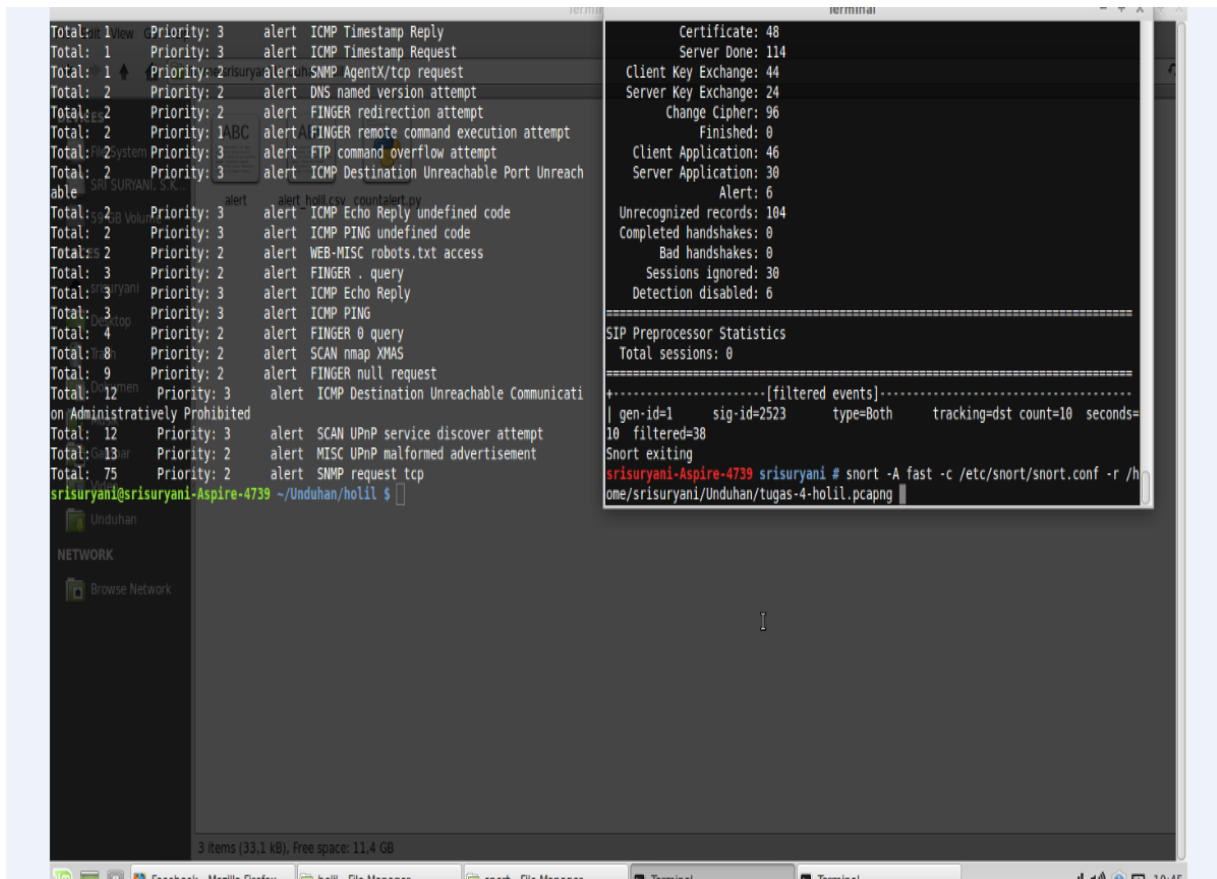
Nama : kholil anggara
Nim : 090111320031

Grafik yan menunjukan alert alert yang diadapatkan , dapat dilihat dibawah ini.



Nama : kholil anggara
Nim : 090111320031

kemudian hasil snort seperti dibawah ini.



```
Total: 1 Priority: 3 alert ICMP Timestamp Reply
Total: 1 Priority: 3 alert ICMP Timestamp Request
Total: 1 Priority: 2 alert SNMP AgentX/tcp request
Total: 2 Priority: 2 alert DNS named version attempt
Total: 2 Priority: 2 alert FINGER redirection attempt
Total: 2 Priority: 1 alert FINGER remote command execution attempt
Total: 2 Priority: 3 alert FTP command overflow attempt
Total: 2 Priority: 3 alert ICMP Destination Unreachable Port Unreach
able
Total: 2 Priority: 3 alert ICMP Echo Reply
Total: 2 Priority: 3 alert ICMP Echo Reply undefined code
Total: 2 Priority: 3 alert ICMP PING undefined code
Total: 2 Priority: 2 alert WEB-MISC robots.txt access
Total: 3 Priority: 2 alert FINGER . query
Total: 3 Priority: 3 alert ICMP Echo Reply
Total: 3 Priority: 3 alert ICMP PING
Total: 4 Priority: 2 alert FINGER 0 query
Total: 8 Priority: 2 alert SCAN nmap XMAS
Total: 9 Priority: 2 alert FINGER null request
Total: 12 Priority: 3 alert ICMP Destination Unreachable Communicati
on Administratively Prohibited
Total: 12 Priority: 3 alert SCAN UPnP service discover attempt
Total: 13 Priority: 2 alert MISC UPnP malformed advertisement
Total: 75 Priority: 2 alert SNMP request tcp
srisuryani@srisuryani-Aspire-4739 ~/Unduhan/holil $

Certificate: 48
Server Done: 114
Client Key Exchange: 44
Server Key Exchange: 24
Change Cipher: 96
Finished: 0
Client Application: 46
Server Application: 30
Alert: 6
Unrecognized records: 104
Completed handshakes: 0
Bad handshakes: 0
Sessions ignored: 30
Detection disabled: 6

=====
SIP Preprocessor Statistics
Total sessions: 0
=====
+-----[filtered events]-----
| gen-id=1 sig-id=2523 type=Both tracking=dst count=10 seconds=
10 filtered=38
Snort exiting
srisuryani-Aspire-4739 srisuryani # snort -A fast -c /etc/snort/snort.conf -r /h
ome/srisuryani/Unduhan/tugas-4-holil.pcapng
```