**INSTRUCTION DETECTION SYSTEM MENGGUNAKAN SNORT**

TUGAS 4

scanning situs target sambil menjalankan wireshark, kemudian compile menggunakan snort, lihat apa yang terjadi?

* Buat table dari hasil alert
* Buat grafiknya
1. Langkah – langkah dilakukan

Scanning target menggunakan Nmap dan Wireshark dengan bersamaan.

Disini saya menggunakan 2 tools : wireshark dan nmap.

* Nmap



Gambar 2.1 Scanning



Gambar 2.2 Scanning

Pada gambar 2.1 saya melakukan scanning terhadap situs target [www.lazada.co.id](http://www.lazada.co.id) dan saya menjalankan aplikasi wireshark bersamaan untuk melihat traffic data yang terjadi saat sedang melakukan scanning.

* wireshark



Gambar 2.2 Scanning

Pada gambar 2.2 diatas merupakan hasil dari traffic di aplikasi wireshark saat melakukan scanning.

* Compile data menggunakan Snort

Setelah kita selesai melakukan scanning di nmap dan mendapatkan data pcap dari wireshak, kita compile file pcap dengan perintah digambar 2.3

snort –A fast –c /etc/snort/snort.conf –r (file pcap data dari wireshark).



Gambar 2.3

Perintah diatas itu untuk mendapatkan hasil alert. Berikut gambar 2.4 hasil alert yang didapatkan.



Gambar 2.4

1. **HASIL DATA**

Setelah mendapatkan data berikut merupakan tampilan dari hasil sajian data alert berupa table dan grafik.

* Table data alert

|  |  |  |
| --- | --- | --- |
| No | Alert | Jumlah |
| 1 | ICMP PING NMAP | 1 |
| 2 | ICMP Timestamp Reply | 1 |
| 3 | ICMP Timestamp Request | 1 |
| 4 | BAD-TRAFFIC 0 ttl | 2 |
| 5 | WEB-CGI finger access | 2 |
| 6 | ICMP Destination Unreachable Protocol Unreachable | 3 |
| 7 | WEB-MISC robots.txt access | 3 |
| 8 | ICMP Destination Unreachable Port Unreachable | 4 |
| 9 | DNS named version attempt | 4 |
| 10 | SNMP AgentX/tcp request | 4 |
| 11 | SNMP request tcp | 4 |
| 12 | ICMP Time-To-Live Exceeded in Transit | 5 |
| 13 | ICMP Echo Reply undefined code | 6 |
| 14 | ICMP PING undefined code | 6 |
| 15 | ICMP Echo Reply | 7 |
| 16 | ICMP PING | 7 |
| 17 | ICMP Destination Unreachable Communication Administratively Prohibited | 8 |
| 18 | ICMP Destination Unreachable Host Unreachable | 8 |
| 19 | COMMUNITY WEB-MISC Proxy Server Access | 24 |
| 20 | SCAN nmap XMAS | 24 |
| 21 | COMMUNITY WEB-MISC mod\_jrun overflow attempt | 30 |
| 22 | BAD-TRAFFIC same SRC/DST | 45 |
| 23 | MISC UPnP malformed advertisement | 421 |
| 24 | SCAN UPnP service discover attempt | 811 |

* Grafik data alert