* **Student packet**:

alert tcp any any -> 192.168.1.1 54321 (msg: "Student Packet"; sid: 1000001;)

|  |  |
| --- | --- |
| Protocol | Tcp |
| src\_ip | - |
| src\_port | - |
| dst\_ip | 192.168.1.1 |
| dst\_port | 54321 |

Prints a message “Student Packet” and is assigned an sid 1000001.



* **Port scan packet**:

alert tcp any any -> 192.168.1.2 [80,443,22,23,21,53,554,1433,3389,1883] (msg: "Port scan Packet"; sid: 1000002;)

|  |  |
| --- | --- |
| Protocol | Tcp |
| src\_ip | - |
| src\_port | - |
| dst\_ip | 192.168.1.2 |
| dst\_port | 80,443,22,23,21,53,554,1433,3389,1883 |

HTTP, HTTPS, SSH, TELNET, FTP, DNS, RTSP, SQL, RDP, MQTT = 80,443,22,23,21,53,554,1433,3389,1883

Prints a message “Port scan packet” and is assigned an sid 1000002.



* **Base64 malicious packet**:

alert tcp any any -> 192.168.1.3 8080 (msg: "Base644 Malicious Packet"; sid: 1000003;)

|  |  |
| --- | --- |
| Protocol | Tcp |
| src\_ip | - |
| src\_port | - |
| dst\_ip | 192.168.1.3 |
| dst\_port | 8080 |

Prints a message “Base644 Malicious Packet” and is assigned an sid 1000003.



* **DNS suspicious domain packet**:

alert udp any any -> 192.168.1.1 53 (msg: "DNS Suspicious Domain Packet"; sid: 1000004;)

|  |  |
| --- | --- |
| Protocol | UDP |
| src\_ip | - |
| src\_port | - |
| dst\_ip | 192.168.1.1 (default dns) |
| dst\_port | 53 |

Prints a message “DNS Suspicious Domain Packet” and is assigned an sid 1000004.



* **Ping test packet**:

alert icmp any any -> 192.168.1.4 any (msg: "Ping Test Packet"; sid: 1000005;)

|  |  |
| --- | --- |
| Protocol | ICMP |
| src\_ip | - |
| src\_port | - |
| dst\_ip | 192.168.1.4 |
| dst\_port | - |

Prints a message “Ping Test Packet” and is assigned an sid 1000005.



**Full console output**:

A screenshot of a computer program

Description automatically generated