Snort Rules

- alert tcp 192.168.0.100 any -> 192.168.1.1 54321 (msg:"Student's Packet Detected"; content:"NAME-ID"; sid:1000001;)

This rule detects packets sent from any source to IP 192.168.1.1 on port 54321 containing the string "NAME-ID".

- alert tcp any any -> 192.168.1.2 80 (msg:"Port Scan Detected - HTTP"; sid:1000002;)

This rule alerts when any traffic is directed to IP 192.168.1.2 on port 80, which is typically used for HTTP.

- alert tcp any any -> 192.168.1.2 443 (msg:"Port Scan Detected - HTTPS"; sid:1000003;)

This rule alerts when any traffic is directed to IP 192.168.1.2 on port 443, which is typically used for HTTPS.

- alert tcp any any -> 192.168.1.2 22 (msg:"Port Scan Detected - SSH"; sid:1000004;)

This rule alerts when any traffic is directed to IP 192.168.1.2 on port 22, which is typically used for SSH.

- alert tcp any any -> 192.168.1.2 23 (msg:"Port Scan Detected - TELNET"; sid:1000005;)

This rule alerts when any traffic is directed to IP 192.168.1.2 on port 23, which is typically used for TELNET.

- alert tcp any any -> 192.168.1.2 21 (msg:"Port Scan Detected - FTP"; sid:1000006;)

This rule alerts when any traffic is directed to IP 192.168.1.2 on port 21, which is typically used for FTP.

- alert tcp any any -> 192.168.1.2 53 (msg:"Port Scan Detected - DNS"; sid:1000007;)

This rule alerts when any traffic is directed to IP 192.168.1.2 on port 53, which is typically used for DNS.

- alert tcp any any -> 192.168.1.2 554 (msg:"Port Scan Detected - RTSP"; sid:1000008;)

This rule alerts when any traffic is directed to IP 192.168.1.2 on port 554, which is typically used for RTSP.

- alert tcp any any -> 192.168.1.2 1433 (msg:"Port Scan Detected - SQL"; sid:1000009;)

This rule alerts when any traffic is directed to IP 192.168.1.2 on port 1433, which is typically used for RTSP.

- alert tcp any any -> 192.168.1.2 3389 (msg:"Port Scan Detected - RDP"; sid:1000010;)

This rule alerts when any traffic is directed to IP 192.168.1.2 on port 3389, which is typically used for RDP.

- alert tcp any any -> 192.168.1.2 1883 (msg:"Port Scan Detected - MQTT"; sid:1000011;)

This rule alerts when any traffic is directed to IP 192.168.1.2 on port 1883, which is typically used for MQTT.

- alert tcp any any -> 192.168.1.3 8080 (msg:"Base64 Malicious Packet Detected"; content:"MTMyNDU2Nzg5MA=="; sid:1000003;)

This rule detects packets sent to IP 192.168.1.3 on port 8080 containing a specific base64-encoded string. The base64 string represents malicious content, possibly indicating an attack or unauthorized data transmission.

- alert udp any any -> any 53 (msg:"Suspicious DNS Query Detected"; sid:1000004;)

This rule flags DNS query traffic on port 53, which is commonly used for domain name resolution.

- alert icmp any any -> 192.168.1.4 any (msg:"Ping Test Packet Detected"; content:"PingTest-2024"; sid:1000005;)

This rule looks for ICMP packets directed to IP 192.168.1.4 containing the string "PingTest-2024".

Screenshot: