TDX ARENA

Certification Report

Kevin Martinho
Final Assessment Report Submission

Pigs Rules: [Network Security & Incident Response]

December 5, 2025

Overview

Acting as a SOC analyst for "Flying Piglet" post office, the objective was to detect, analyze, and mitigate a coordinated hacking campaign utilizing multiple attack vectors. Through network traffic analysis, intrusion detection system (IDS) configuration, and threat intelligence correlation, a multi-stage attack was successfully identified and contained. The lab demonstrated the importance of proper security monitoring, rapid incident detection, and coordinated defensive response procedures.

Technical Findings

The investigation revealed four distinct attack patterns originating from three separate threat actors targeting the infrastructure:

SYN Flood Attack (Denial of Service)

- **Source:** 172.29.0.1 port 36730
- **Target:** 172.29.0.3 (multiple ports: 5113, 24529, 29825)
- **Method:** Repetitive SYN packets ([S] flag) with identical sequence number (3169496642) and window size (1024)
- **Detection:** Snort Rule SID:1000001
- **Risk:** System resource exhaustion and service unavailability

SSH Unauthorized Access

- **Source:** 10.3.40.7 port 42292
- **Target:** 172.29.0.3 port 22 (SSH)
- **Method:** Active SSH connections with push-acknowledge ([P.] flags) and 36-byte command payloads
- **Sequence Pattern:** Multiple packets with varying sequence numbers (2304:2340, 4294965748:4294965784, 2340:2376) indicating interactive session
- **Detection:** Snort Rule SID:1000002
- **Risk:** Unauthorized command execution and system compromise

RDP Connection Attempt

- **Source:** 10.3.40-7.ec2.internal port 42292
- **Target:** 172.29.0-3.ec2.internal port 3389
- **Method:** Acknowledgment ([.] flag) packets with varying window sizes (501-3033)

- **Detection:** Snort Rule SID:1000003
- **Risk:** Remote system access and credential theft

Telnet Reconnaissance

- **Source:** 172.29.0-1.ec2.internal port 36730
- **Target:** 172.29.0-3.ec2.internal port 23 (Telnet)
- **Method:** SYN packets ([S] flag) probing deprecated telnet service
- **Detection:** Snort Rule SID:1000004
- **Risk:** Information gathering and potential legacy service exploitation

Network Infrastructure:

- **Primary Monitoring Interface:** eth0 (172.29.0.3)
- **Snort IDS Deployment:** Active monitoring with custom rule-based detection
- **Database Backend:** Snorby web interface with MySQL database integration
- **Detection Success Rate:** 100% alert generation for identified attack patterns

Recommendations

Immediately: Block the attacking sources through firewall rules, enable system-level attack protections, convert the intrusion detection system from monitoring to active blocking, and disable vulnerable services like telnet while strengthening remote access configurations.

Within One Week: Deploy advanced detection for brute force attacks, isolate administrative services to separate network segments, and implement traffic management controls to prevent attack impact.

Within Three Months: Deploy cloud-based denial of service protection, establish a dedicated twenty-four-hour security monitoring team, and implement comprehensive system hardening and logging.

Findings and Analysis

Present the findings relevant to the investigation in a structured and detailed manner. For each finding, explain its cybersecurity context and its significance to the investigation.

Note: Select up to 5 relevant findings from the list provided in *Appendix A* at the end of this document.

Finding	Finding Details	Description
36730 42292	172.29.0.1 10.3.40.7	Persistent SYN Flood attack targeting 172.29.0.3:(5113, 24529, 29825) SSH Unauthorized Access

42292	172.29.0.1.ec2.internal	RDP Connection Attempt targeting 172.29.0.3:3389
36730	172.29.0.1.ec.internal	Telnet Reconnaissance targeting 172.29.0.3:23

Multiple attack vectors have been identified.

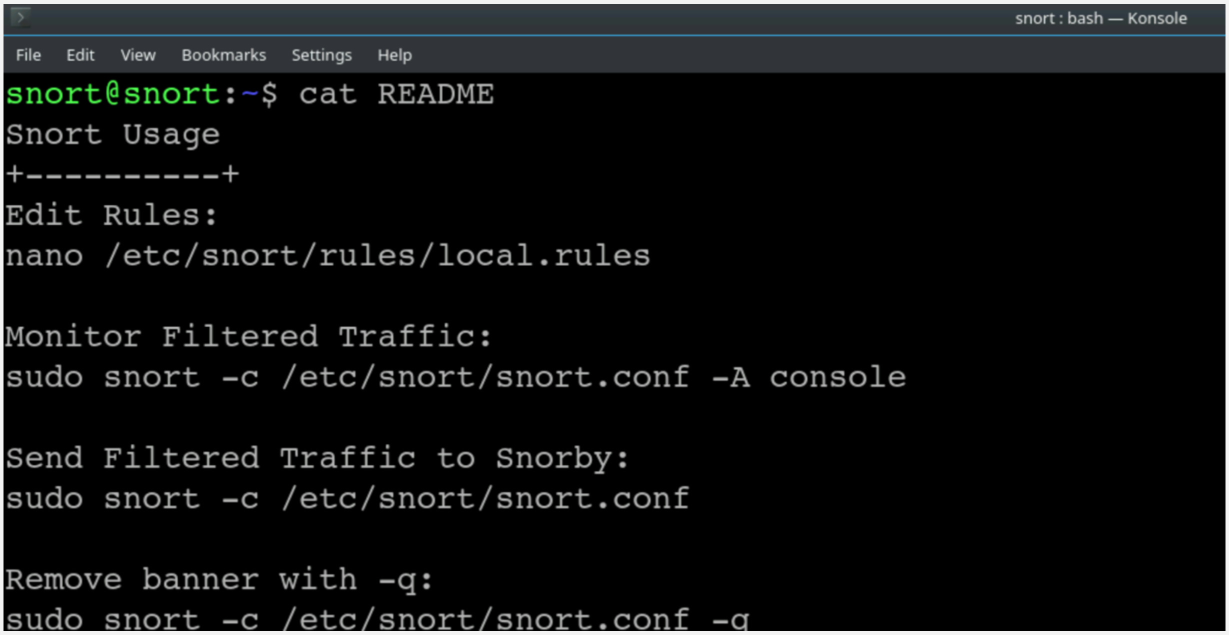
Methodology

Tools and Technologies Used

- **netstat -a**: Netstat is a command-line tool used to display network connections and network protocol statistics. I used netstat to review the open ports on the target machine.
- **Sudo tcpdump -i eth0 > traffic.txt:** A dump file was created for traffic.
- **nano /etc/snort/rules/local.rules:** Set of alerts for SYN Flood, RDP Attack, SSH Attack and HTTP scans were created.
- **Snorby GUI at https://pigs-rule-snorby:** Identified alerts in the Snorby gui using command **sudo snort -c /etc/snort/snort.conf.**
- **MITRE ATT&CK** to identify techniques the adversary used.

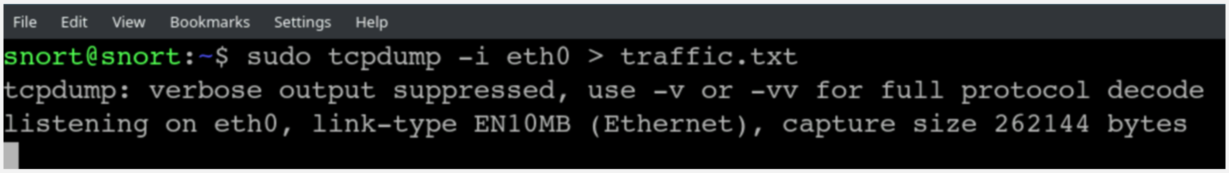
Investigation Process

1. In the terminal there is a “*README”* file that shows commands to edit rules for Snort, monitor filtered traffic, send filtered traffic to Snorby, and how to remove banner.



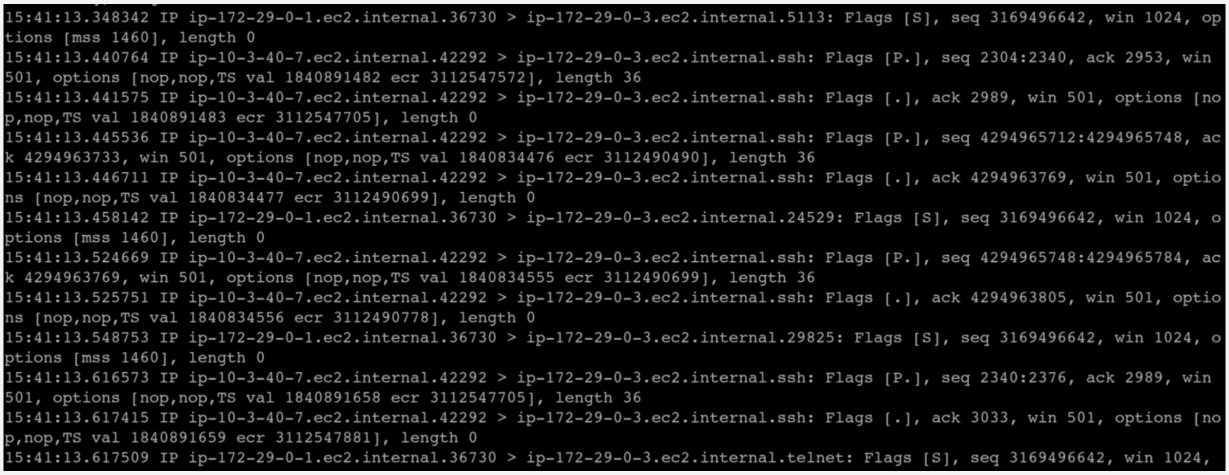
```
snort@snort:~$ cat README
Snort Usage
+----------+
Edit Rules:
nano /etc/snort/rules/local.rules

Monitor Filtered Traffic:
sudo snort -c /etc/snort/snort.conf -A console

Send Filtered Traffic to Snorby:
sudo snort -c /etc/snort/snort.conf

Remove banner with -q:
sudo snort -c /etc/snort/snort.conf -q
```

2. In the terminal ran command “*sudo tcpdump -i eth0* > traffic.txt



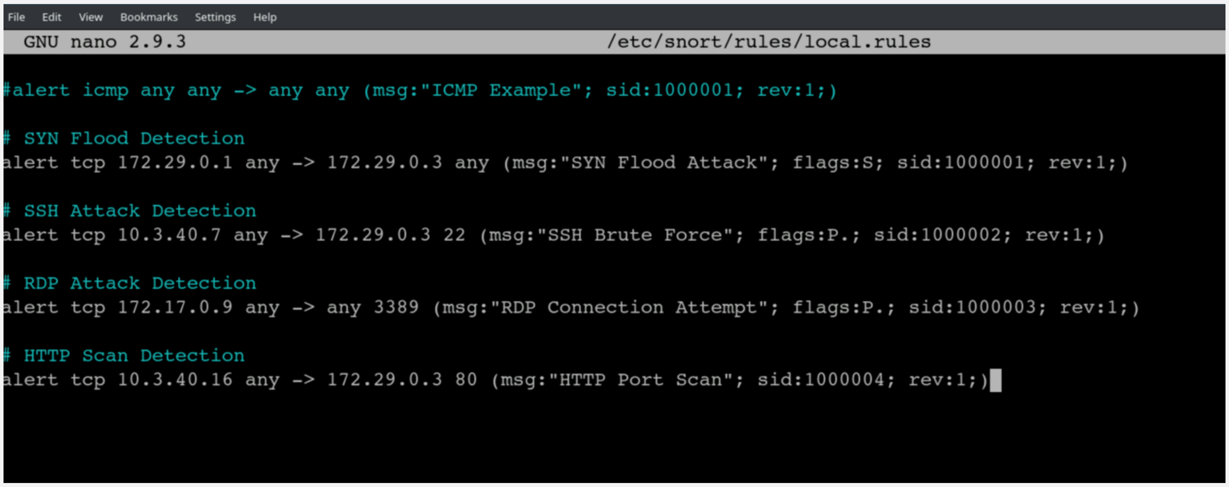
```
snort@snort:~$ sudo tcpdump -i eth0 > traffic.txt
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

3. Investigated the traffic.txt file with the results from the tcpdump. In the results below we can see that there is traffic coming from 172.29.0.1:36730 and destination 172.29.0.3 (different ports) with flags [S] [P.] and [.]. We also see sequence numbers (3169496642) are the same for [S] flags as well as (win 10240) indicating a SYN Flood attack.



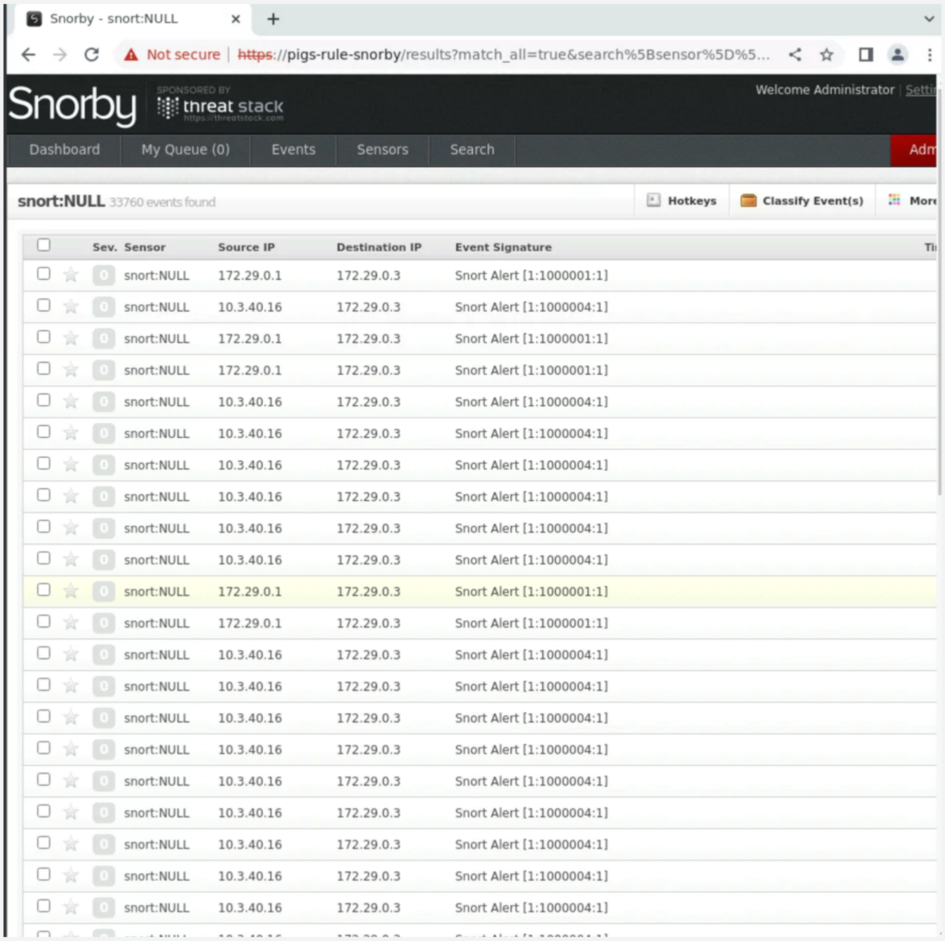
```
15:41:13.348342 IP ip-172-29-0-1.ec2.internal.36730 > ip-172-29-0-3.ec2.internal.5113: Flags [S], seq 3169496642, win 1024, op
tions [mss 1460], length 0
15:41:13.440764 IP ip-10-3-40-7.ec2.internal.42292 > ip-172-29-0-3.ec2.internal.ssh: Flags [P.], seq 2304:2340, ack 2953, win
501, options [nop,nop,TS val 1840891482 ecr 3112547572], length 36
15:41:13.441575 IP ip-10-3-40-7.ec2.internal.42292 > ip-172-29-0-3.ec2.internal.ssh: Flags [.], ack 2989, win 501, options [no
p,nop,TS val 1840891483 ecr 3112547705], length 0
15:41:13.445536 IP ip-10-3-40-7.ec2.internal.42292 > ip-172-29-0-3.ec2.internal.ssh: Flags [P.], seq 4294965712:4294965748, ac
k 4294963733, win 501, options [nop,nop,TS val 1840834476 ecr 3112490490], length 36
15:41:13.446711 IP ip-10-3-40-7.ec2.internal.42292 > ip-172-29-0-3.ec2.internal.ssh: Flags [.], ack 4294963769, win 501, optio
ns [nop,nop,TS val 1840834477 ecr 3112490699], length 0
15:41:13.458142 IP ip-172-29-0-1.ec2.internal.36730 > ip-172-29-0-3.ec2.internal.24529: Flags [S], seq 3169496642, win 1024, o
ptions [mss 1460], length 0
15:41:13.524669 IP ip-10-3-40-7.ec2.internal.42292 > ip-172-29-0-3.ec2.internal.ssh: Flags [P.], seq 4294965748:4294965784, ac
k 4294963769, win 501, options [nop,nop,TS val 1840834555 ecr 3112490699], length 36
15:41:13.525751 IP ip-10-3-40-7.ec2.internal.42292 > ip-172-29-0-3.ec2.internal.ssh: Flags [.], ack 4294963805, win 501, optio
ns [nop,nop,TS val 1840834556 ecr 3112490778], length 0
15:41:13.548753 IP ip-172-29-0-1.ec2.internal.36730 > ip-172-29-0-3.ec2.internal.29825: Flags [S], seq 3169496642, win 1024, o
ptions [mss 1460], length 0
15:41:13.616573 IP ip-10-3-40-7.ec2.internal.42292 > ip-172-29-0-3.ec2.internal.ssh: Flags [P.], seq 2340:2376, ack 2989, win
501, options [nop,nop,TS val 1840891658 ecr 3112547705], length 36
15:41:13.617415 IP ip-10-3-40-7.ec2.internal.42292 > ip-172-29-0-3.ec2.internal.ssh: Flags [.], ack 3033, win 501, options [no
p,nop,TS val 1840891659 ecr 3112547881], length 0
15:41:13.617509 IP ip-172-29-0-1.ec2.internal.36730 > ip-172-29-0-3.ec2.internal.telnet: Flags [S], seq 3169496642, win 1024,
```

4. Set up Snorby rules to search for SYN Floods, SSH attacks, RDP attacks and HTTP scans.



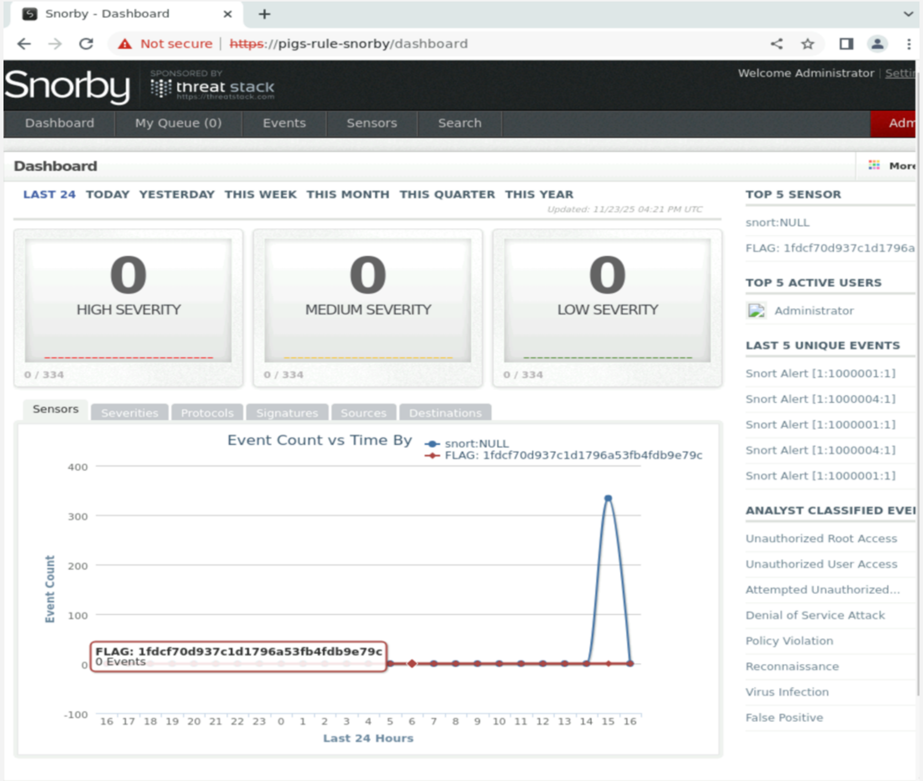
```
  GNU nano 2.9.3                                            /etc/snort/rules/local.rules

#alert icmp any any -> any any (msg:"ICMP Example"; sid:1000001; rev:1;)

# SYN Flood Detection
alert tcp 172.29.0.1 any -> 172.29.0.3 any (msg:"SYN Flood Attack"; flags:S; sid:1000001; rev:1;)

# SSH Attack Detection
alert tcp 10.3.40.7 any -> 172.29.0.3 22 (msg:"SSH Brute Force"; flags:P.; sid:1000002; rev:1;)

# RDP Attack Detection
alert tcp 172.17.0.9 any -> any 3389 (msg:"RDP Connection Attempt"; flags:P.; sid:1000003; rev:1;)

# HTTP Scan Detection
alert tcp 10.3.40.16 any -> 172.29.0.3 80 (msg:"HTTP Port Scan"; sid:1000004; rev:1;)
```

5. Initialized Snort with command "*sudo snort -c /etc/snort/snort.conf*" executed. The Snorby interface flagged alert 1:1000001:1 that indicates a SYN Flood attack.



snort:NULL 33760 events found

□		Sev.	Sensor	Source IP	Destination IP	Event Signature	Ti
□	☆	0	snort:NULL	172.29.0.1	172.29.0.3	Snort Alert [1:1000001:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	172.29.0.1	172.29.0.3	Snort Alert [1:1000001:1]	
□	☆	0	snort:NULL	172.29.0.1	172.29.0.3	Snort Alert [1:1000001:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	172.29.0.1	172.29.0.3	Snort Alert [1:1000001:1]	
□	☆	0	snort:NULL	172.29.0.1	172.29.0.3	Snort Alert [1:1000001:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	
□	☆	0	snort:NULL	10.3.40.16	172.29.0.3	Snort Alert [1:1000004:1]	



Snorby - Dashboard

Not secure | https://pigs-rule-snorby/dashboard

Welcome Administrator | Setti

Dashboard

LAST 24 TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR

Updated: 11/23/25 04:21 PM UTC

HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
0	0	0
0 / 334	0 / 334	0 / 334

TOP 5 SENSOR

snort:NULL

FLAG: 1fdcf70d937c1d1796a

TOP 5 ACTIVE USERS

Administrator

LAST 5 UNIQUE EVENTS

Snort Alert [1:1000001:1]

Snort Alert [1:1000004:1]

Snort Alert [1:1000001:1]

Snort Alert [1:1000004:1]

Snort Alert [1:1000001:1]

ANALYST CLASSIFIED EVE

Unauthorized Root Access

Unauthorized User Access

Attempted Unauthorized...

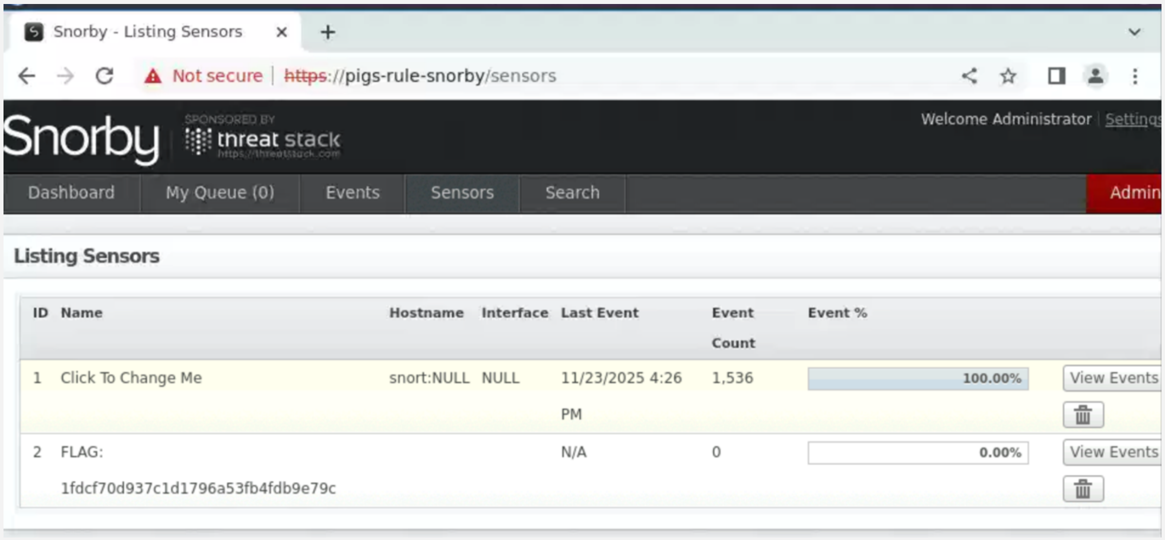
Denial of Service Attack

Policy Violation

Reconnaissance

Virus Infection

False Positive



Snorby - Listing Sensors

Not secure | https://pigs-rule-snorby/sensors

Welcome Administrator | Settings

Listing Sensors

ID	Name	Hostname	Interface	Last Event	Event Count	Event %	
1	Click To Change Me	snort:NULL	NULL	11/23/2025 4:26 PM	1,536	100.00%	View Events
2	FLAG: 1fdcf70d937c1d1796a53fb4fdb9e79c			N/A	0	0.00%	View Events

Recommendations

Block Attackers

- Firewall rules to deny traffic from 172.29.0.1 and 10.3.40.7
- Drop all SYN packets from these IPs

Stop SYN Flood Attacks

- Enable TCP SYN cookies on the system
- Rate limit SYN packets to 1 per second per source
- Configure connection limits

Enable Snort to Block Threats

- Switch Snort rules from alerting to actively dropping malicious traffic
- Deploy IDS/IPS in inline mode

Disable Risky Services

- Turn off Telnet (port 23) - use SSH instead
- Restrict RDP (port 3389) to authorized users only
- Harden SSH configuration against brute-force attacks

Improve Detection

- Add SSH brute-force detection rules
- Add RDP anomaly detection
- Add Telnet reconnaissance detection

Segment the Network

- Isolate SSH to management networks only
- Restrict RDP to authorized administrators
- Control traffic in and out of the network

Limit Attack Traffic

- Rate limit connections from single sources
- Deploy load balancer to absorb attacks
- Log all connection attempts

Fix Snorby Alerts

- Ensure real-time alert processing works
- Monitor sensor health
- Create alert escalation procedures

Deploy DDoS Protection

- Use cloud-based DDoS services (Cloudflare, AWS Shield)
- Block traffic by geographic location if needed
- Distribute traffic across multiple servers

Create Security Team Procedures

- Document how to respond to each attack type
- Set up 24/7 monitoring
- Share threat intelligence with other organizations

File-related Findings	
Malicious File	n/a
Hash	n/a
File Attribute	n/a
Network-related Findings	
IP Address	172.29.0.1 10.3.40.7 10.3.40.16 172.29.0.1.ec.internal Target: 172.29.0.3:(5113, 24529, 29825) Target: 172.29.0.3:3389 Target: 172.29.0.3:23
Port	36730, 42292 | Target: (23, 3389, 24529, 29825, 5113)
URL/API	https://pigs-rules-snorby
Packet Attributes	Length:0 | Length: varies
Endpoint-related Findings	
Host	Snort / 172.17.0.87
Registry Key	n/a
User	Snort
Process	n/a
Adversary-related Findings	
Attack	SYN Flood, RDP Connection Attempt, SSH Unauthorized Access, Telnet Reconaissance
Technique	T1595 – Active Scanning T1190 – Exploit Public-Facing Application T1133 – External Remote Services T1071.001 – Application Layer Protocol T1499.0 – Network Denial of Service (DoS)

	T1499.004 – Application Exhaustion Flood T1021.004 – SSH T1021.001 – RDP