INFOTACT SOLUTION

# Snort Detection Rules and Attack Simulation Report

Submitted by: Mohamed Nabil Abdul Rahiman

Date: July 27, 2025

## Week 1: Snort Rules Development and Configuration

1. In-depth Snort Rule Syntax:  
Snort rules consist of a rule header and options:  
Syntax: action proto src\_ip src\_port -> dest\_ip dest\_port (options)  
  
Example:  
alert tcp any any -> 192.168.1.0/24 80 (msg:"HTTP traffic detected"; sid:1000001; rev:1;)

2. Custom Detection Rules:  
Rule 1: Detect DNS query for a malicious domain  
alert udp any any -> any 53 (msg:"Suspicious DNS query for badsite.com"; content:"badsite.com"; nocase; sid:1000002; rev:1;)  
  
Rule 2: Detect FTP login attempt  
alert tcp any any -> any 21 (msg:"FTP login attempt detected"; flow:to\_server,established; content:"USER "; nocase; sid:1000003; rev:1;)

3. Integration into Snort Configuration:  
- Rules added to /etc/snort/rules/local.rules  
- Included in /etc/snort/snort.conf  
- Configuration tested with: snort -T -c /etc/snort/snort.conf

## Week 2: Attack Simulation and Alert Verification

1. Simulated Attacks:  
- TCP Port Scan using: nmap -sS [target IP]  
- SSH Brute Force simulated with Hydra: hydra -l root -P passwords.txt ssh://[target IP]  
  
2. Alert Verification:  
- Verified alerts generated by Snort for port scans and brute force attempts  
- Rules triggered successfully as expected  
  
3. Detection Quality Analysis:  
- Port scan and brute force activity successfully logged  
- Alerts matched correct protocols, ports, and IPs

## Week 3: False Positives and Rule Tuning

1. Identified False Positives:  
- Some legitimate FTP traffic triggered false alerts  
- DNS traffic to trusted domains incorrectly flagged  
  
2. Suppressed Noisy Rules:  
- Used suppression list in threshold.conf or refined rule content matching  
  
3. Fine-tuning Rules:  
- Adjusted content matching with stricter patterns  
- Added IP/port filters to narrow detection scope

## Week 4: Final Report Compilation

This report covers:  
- Custom Snort rules for DNS and FTP detection  
- Configuration and integration process  
- Simulated attacks including TCP port scan and SSH brute force  
- Alert validation and quality analysis  
- False positive mitigation and rule adjustments  
  
INFOTACT SOLUTION project successfully demonstrates intrusion detection using Snort.