

Title: Unauthorized Service Detection using Port & Process Monitoring

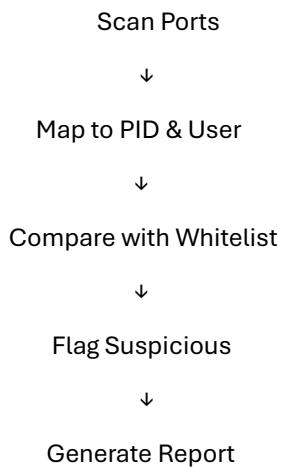
Scenario: A server should run only approved services.

If an unknown port is open, it may be unauthorized or malicious.

Use Case: The tool checks open ports, maps them to processes and users, compares with an approved list, and flags suspicious services.

Objective: To detect unauthorized services and generate a security report.

Process: First we scan open ports, map them to processes and users, validate them against a whitelist, and finally generate a security audit report.”



STEP 1: Scan Ports

Get all active listening ports from system

Store in PORT_LIST

STEP 2: Map to PID & User

FOR each PORT in PORT_LIST:

 Get PID using that PORT

 Get PROCESS_NAME using PID

 Get USER running the process

STEP 3: Compare with Whitelist

IF PORT exists in WHITELIST:

 Mark as APPROVED

ELSE:

 Mark as SUSPICIOUS

 Add to SUSPICIOUS_LIST

STEP 4: Flag Suspicious

IF SUSPICIOUS_LIST is not empty:

 Display warning message

ELSE

Display "All ports are authorized"

STEP 5: Generate Report

Print Date and Time

Print Approved Ports

Print Suspicious Ports

Save report to file (optional)