CSE 115A – Introduction to Software Engineering Test Plan and Report:

Product: SlugShield – Intrusion Detection Tool

Team: Andy Liu, Anish Talluri, Jace Chambers, Asaveri Rao

Scenario 1 - ICMP flood Detection (Pass)

Related user story: User Story 1 – I want to detect ICMP flood attacks

1. Started backend with python run_backend.py
2. Ran python /tools/simulate_icmp_flood.py
3. Watched backend logs in recent alert panel
4. Checked and configured alert email inbox

We observed that the expected ICMP flood alerts in logs and on the dashboard without crashes or errors, making it so that this scenario passed.

Scenario 2 - ARP Spoofing Detection (Pass)

Related user story 2- I want to detect ARP spoofing

1. Started backend with python run_backend.py
2. Ran python /tools/simulate_arp_spoof.py which sends baseline ARP traffic with an attack phase with Mac changes for a single IP
3. Watched backend logs and dashboard alerts list
4. Checked email inbox for Arp-related alerts

NO alerts during baseline, and a clear ARP spoof alert during the attack phase, so this passes

Scenario 3 - Port Scan Detection (Pass)

Related user story: User Story 3 – I want to detect port scans

1. Started backend with python run_backend.py
2. Ran python tools/simulate_port_scan.py which sends baseline traffic followed by a burst of SYNs to many ports
3. Monitored backend logs and dashboard alerts for a port-scan detection
4. Checked email inbox for port-related alerts

Baseline did not produce an alert, and the scan phase produced a port-scan alert as expected, thus it is considered passing

Scenario 4 - SSH Brute-Force Detection (Pass)

Related user story: User Story 4 - Detect SSH brute-force attempts

1. Started backend with python run_backend.py
2. Ran python tools/simulate_ssh_detections.py which sends normal SSH traffic, then a burst of brute force attempts.
3. Monitored backend logs and dashboard alerts
4. Check email inbox for ssh-related alerts

Only brute-force phase triggered an alert which matches the configured thresholds, meaning that it passed.

Scenario 5 - Light/Dark Mode (Pass)
Related user story: User Story 5 - I want to switch between light and dark mode so that the dashboard can be read in both times of the day.

1. Start the frontend and open dashboard in a browser
2. Use the Light/Dark mode toggle within the UI

Users can toggle between Light and Dark mode and both modes are readable.

Scenario 6 - Adjusting Detector Thresholds (Pass)
Related user story: User Story 6 - I want to adjust detection thresholds so that I can control the sensitivity to suspicious traffic.

1. Start backend and open dashboard
2. Locate threshold control
3. Change threshold value and confirm new value is in UI

Detector thresholds update from the UI and alerts are accordingly changed.

Scenario 7 - Email notifications for Alerts (Pass)
Related user story: User Story 7 - I want to receive email notifications whenever an alert is detected.

1. Start backend and dashboard
2. Trigger an alert using one of the simulation scripts using an endpoint.
3. Confirm alert appears in dashboard
4. Confirm email inbox, and verify alert email arrived.

Each new alert generates an email notification meaning that it passed.

Scenario 8 -Viewing Recent Alerts (Pass)
Related user story: User Story 8 - I want to see a clear list of recent alerts so that I can understand what has happened on my network.

1. Start backend and Open dashboard
2. Trigger one test alert
3. Verify that alert appears on dashboard

Recent alerts show the latest alerts first, showing what happened, and it persists when the page reloads.