

Homework

Three tasks to extend the network-traffic lab into a repeatable hunting workflow.

Finish the lab first. Cross-reference with [answer.html](#) after you submit.

Task 1 — Beacon Hunting Script

Objective

Automate the beacon detection you did manually in Exercise 4.

Instructions

1. Write a Python script that takes a NetFlow CSV and groups flows by `(src, dst, dport)` tuple.
2. For each tuple, compute inter-flow intervals, mean, stddev, and jitter percentage.
3. Emit any tuple with jitter $< 30\%$ and at least 5 flows as a candidate beacon.

Deliverable

`beacon_hunt.py` and its output when run against the lab NetFlow file.

Task 2 — DNS Exfil Decoder

Objective

Build a reusable decoder for DNS-tunneled data.

Instructions

1. For each query in the DNS log that matches the pattern "base32/64 subdomain under a single second-level domain", extract and concatenate the leftmost labels.
2. Attempt base32 and base64 decoding, print whichever yields printable text.
3. If the decoded content looks like a multipart payload, reassemble in order.

Deliverable

`dns_decode.py` with tested output against the lab file.

Task 3 — Egress Filter Recommendation

Objective

Turn your lab findings into a firewall rule proposal.

Instructions

1. Based on the C2 channel identified in Exercise 4, draft five egress firewall rules that would have blocked the beacon without breaking legitimate traffic.
2. Each rule: action, direction, source, destination, port, protocol, business justification.
3. For each rule, estimate the false-positive risk (which legitimate application might also be affected?).

Deliverable

A markdown file `egress-rules.md`.