Zeek Exercises

## 🔍 **Zeek Exercises - Summary Notes**

### ✅ **Objective**

Practice using **Zeek logs**, custom **signatures**, and **scripts** to analyze network traffic and detect threats.

### 🔹 **Exercise 1: Analyzing Zeek Logs**

* Use conn.log, dns.log, http.log, and ssl.log.
* Commands:
  + cat conn.log | zeek-cut id.orig\_h id.resp\_h proto
  + zeek-cut id.orig\_h id.resp\_h id.resp\_p < conn.log | sort | uniq -c | sort -nr
* Skills:
  + Filter connections by IP/port
  + Identify unusual traffic (e.g., external IPs on suspicious ports)

### 🔹 **Exercise 2: DNS Log Analysis**

* Use dns.log to identify:
  + Domains being queried
  + Suspicious or known-malicious domains
* Useful fields:
  + query, qtype\_name, rcode\_name
* Command example:

bash

CopyEdit

cat dns.log | zeek-cut query qtype\_name rcode\_name | sort | uniq -c | sort -rn

### 🔹 **Exercise 3: HTTP Log Inspection**

* Focus on http.log
* Extract:
  + host, uri, user\_agent, status\_code
* Look for:
  + Suspicious user-agents or download activity
  + Unusual HTTP methods (PUT, DELETE)
* Example:

bash

CopyEdit

cat http.log | zeek-cut host uri method user\_agent

### 🔹 **Exercise 4: Signature-based Detection**

* Create a simple .sig file to detect patterns (e.g., strings or known shell commands)
* Example:

zeek

CopyEdit

signature test\_http\_get {

ip-proto == tcp

payload /GET \/evil/

event "Detected malicious HTTP GET request"

}

* Place in local.sig, and enable in local.zeek:

zeek

CopyEdit

@load ./local.sig

### 🔹 **Exercise 5: Writing Basic Zeek Scripts**

* Create custom event handlers:

zeek

CopyEdit

event connection\_established(c: connection) {

print fmt("Connection from %s to %s", c$id$orig\_h, c$id$resp\_h);

}

* Save in a .zeek file and run:

bash

CopyEdit

zeek -r traffic.pcap custom\_script.zeek

### 🔹 **Exercise 6: Using Zeek Packages**

* Install and run external Zeek packages:

bash

CopyEdit

zkg install zeek/zeek-package-name

zeek -r capture.pcap --scripts=/path/to/package

### 📌 **Tips**

* Zeek processes PCAP files with zeek -r file.pcap
* Use zeek-cut to extract fields from log files
* Always check notice.log and weird.log for anomalies
* Use site/local.zeek to customize and load scripts or signatures

