Frage (2Pkt)

Ex1 - Select all true statements about “Active Information Gathering” (more than one right answer is possible):

[ ] “Using Netcraft to know about who is hosting the webserver of a targeted company” is an example of Active Information Gathering.

[ ] Several Active Information Gathering methods can be detected by the target.

[ ] Active Information Gathering is always illegitimate.

[ ] “Using Ping to check if a targeted IP address is responsive” is an example of Active Information Gathering .

> false, true, false, true

Frage (3Pkt)

Ex1 - In a “Brute Force” attack for guessing a password, we usually would see (more than one right answer is possible):

[ ] One source IP sending many packets with different payloads to a single destination IP in a short time.

[ ] Many different source IPs sending only one or two TCP SYN packets to the same destination IP in a short time.

[ ] One source IP sending one or two TCP SYN packets to many different destination IPs in a short time.

[ ] One source IP sending one TCP SYN packet to many different Ports of the same destination IP in a short time.

> true, false, false, false

Frage (3Pkt)

Ex2 - Select all true statements about the extraction of network traffic flows (more than one right answer is possible). Given a pcap captured in a normal backbone network...

[ ] If the defined flow timeout is 10 seconds, I will probably get more flows than if the defined flow timeout is 10 minutes.

[ ] If flows are extracted with a 2-tuple key: <SrcIP, DstIP>, I will probably get more flows than if extracted with a 5-tuple key: <SrcIP, DstIP, SrcPort, DstPort, Protocol>.

[ ] If flows are extracted “bidirectional”, I will probably get more flows than if extracted “one-directional”.

[ ] The number of flows will be probably lower than the number of sent packets.

> true, false, false, true

Frage (3Pkt)

Ex3 - Select all true statements about the Darkspace data that we analyzed in the lab (in which IP address scanning activities stand for a majority of captured traffic). In a traffic capture (pcap) of the Darkspace...

[ ] The number of unique IP sources was similar to the number of unique IP destinations.

[ ] We could not make any statement about the relationship between the number of unique IP sources and the number of unique IP destinations.

[ ] The number of unique IP sources was considerably lower than the number of unique IP destinations.

[ ] The number of unique IP sources was considerably higher than the number of unique IP destinations.

> false, false, true, false

Frage (2Pkt)

Ex3 - Select all true statements about Boxplots (more than one right answer is possible):

[ ] Default (or most common) boxplots do not show the mean.

[ ] Boxplots always show outliers.

[ ] Boxplots usually show data percentiles (e.g., quartiles).

[ ] Boxplots provide more detailed information about the distribution of random variables than histograms.

> true, false, true, false

Frage (3Pkt)

Ex3 - Select all true statements (more than one right answer is possible). Given the time series and its corresponding FFT shown in Fig. 1, and taking into account that period = n / k, where n is the number of samples (n = 676).

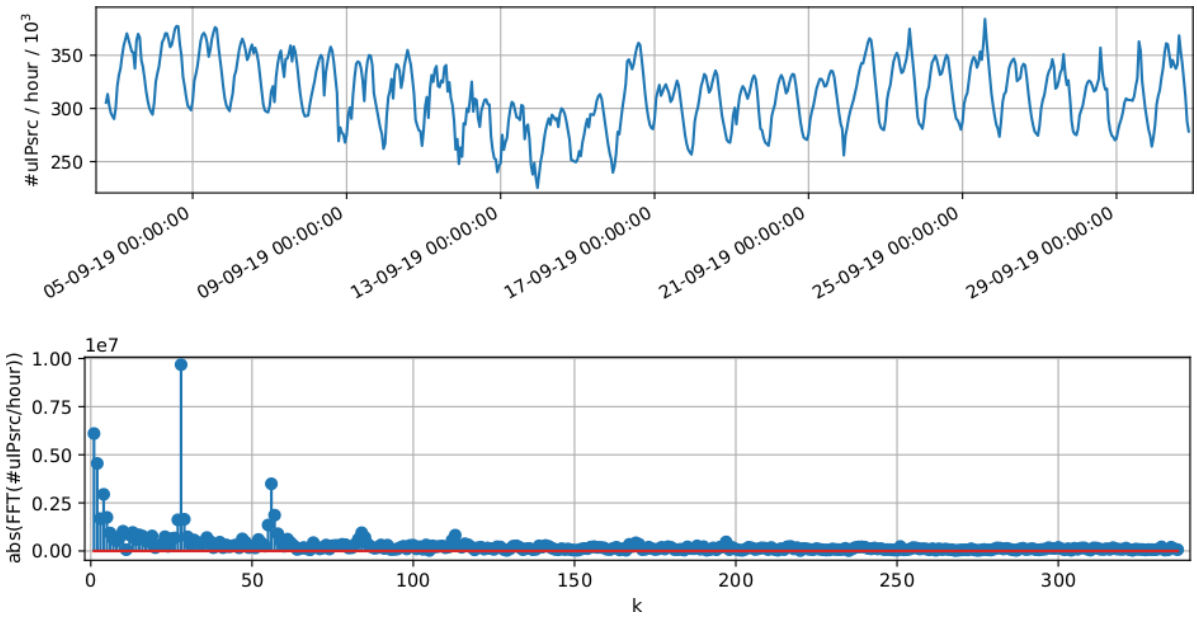

Fig. 2. x: Number of Unique IPsrc/hour (upper), FFT(x) (lower).

[ ] The FFT plot (lower plot) cannot correspond to the time series plot (upper), i.e., peaks in the FFT and shapes in the time series are completely unrelated.

[ ] The peak in k=28 marks an approx. half-day pattern and the peak in k=56 marks and approx. daily pattern.

[ ] The peak in k=28 marks an approx. daily pattern and the peak in k=56 marks and approx. half-day pattern.

[ ] High values on the left of the FFT signal (lower plot) indicate long-term repetition patterns (i.e., large periods) in the time series (upper).

> false, false, true, true

Frage (2Pkt)

Ex4 - We use a scatter plot (x-axis: IP sources, y-axis: IP destinations) to show traffic related to a server being attacked with many SYN requests from spoofed addresses (and the server is not responding). Select the true statement:

[ ] We will see dots drawing a diagonal line.

[ ] We will see dots drawing a vertical line.

[ ] We will see dots drawing a horizontal line.

[ ] We will see one dot (or a cluster/cloud of dots if we use some jitter).

> false, false, true, false

Frage (2Pkt)

Ex4 - When we plot the histogram of TTLs of a bunch of captured packets in a network, we commonly see a figure with some mountain shapes (i.e., multi-modal shapes). Check the true statements (more than one right answer is possible):

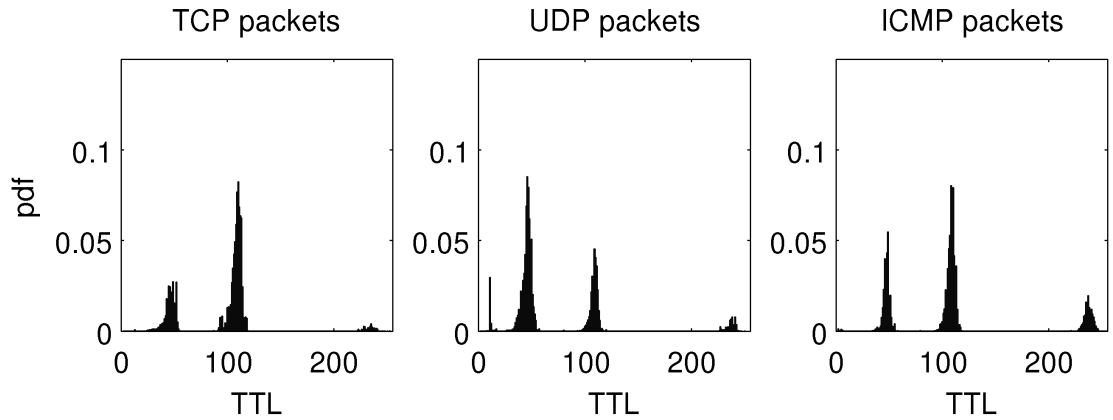

Fig. 3. Some examples of mountain or multi-modal shapes in TTL histograms.

[ ] All the three other answers are wrong.

[ ] The number of mountains is related to the number of hops that packets make in the network.

[ ] The number of mountains is useful to identify the different operating systems that packet senders use.

[ ] The number of mountains gives a relation of the number of IP destinations that IP sources are communicating with on average.

> false, false, true, false