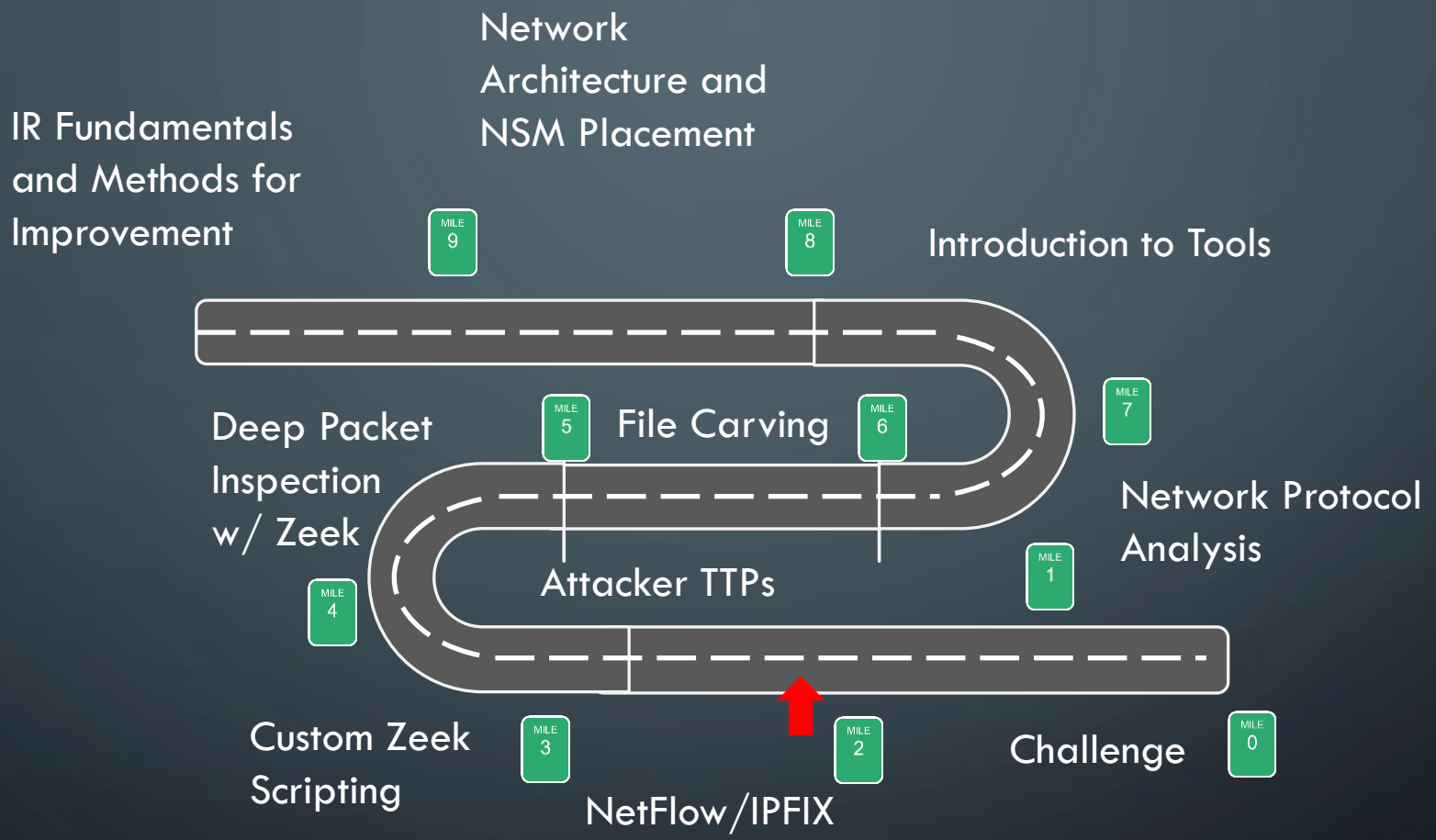
NETWORK FORENSICS & INCIDENT RESPONSE

w/ Troy Wojewoda

DAY 4

Roadmap



IPFIX/Netflow

- Cisco Netflow Version 9
  - IETF standard known as IP Flow Information Export (IPFIX)
- Exporter/Collector architecture
  - Exporter: Routers and Layer-3 switches
  - Collector: Centralized server that receives exporter data
- Exporter outputs flow record when session is over
  - Configurable, can have fixed intervals
- Common record data
  - Src/Dst IP Addresses
  - IP Protocol
  - Src/Dst Layer-4 Port Numbers
  - Number of Bytes and Packets observed
  - TCP Flags Observed (if applicable)
  - Next-Hop address (layer-3 routing)
  - Autonomous System (AS) number of observed IP addresses
  - Much more…

Yaf

YAF – Yet Another Flowmeter

- Processes network traffic from either PCAP files or a network interface and converts to bidirectional flows – exports to IPFIX
- Output can be used with:
  - SiLK
  - super_mediator
  - Pipeline 5

https://tools.netsa.cert.org/yaf/docs.html

https://tools.netsa.cert.org/index.html

Yaf – Field Names

start-time: Start time of the flow

end-time: End time of the flow

duration: Flow duration in fractional seconds. Only present if the flow has a non-zero duration

rtt: Round-trip time estimate in milliseconds in decimal format

proto: IP protocol identifier in decimal format

(sip|dip): Source|Destination IPv4 address in dotted-quad format or IPv6 address in RFC 2373 format

(sp|dp): Source|Destination transport port in decimal format

(pkt|rpkt): Forward|Reverse first-packet 802.1q VLAN tag in hexadecimal format

(oct|roct): Forward|Reverse octet count in decimal format (number of bytes)

Yaf – Field Names (cont.)

(iflags|riflags|uflags|ruflags): Forward|Reverse first-packet TCP flags; forward|reverse nth-packet TCP flags union; where each flags bit is represented by the first character in the flag's name: FIN, SYN, RST, PSH, ACK, URG, ECE, CWR. The character 0 means no flags are set (and will appear in the nth-packet field for single-packet TCP flows).

(isn|risn): Forward|Reverse initial TCP sequence number in hexadecimal format.

(tag|rtag): Forward|Reverse first-packet 802.1q VLAN tag in hexadecimal format.

app: The application label, if *yaf* was built with application labeling enabled and the application labeler was able to identify the payload in the flow.

Yaf – Field Names (cont.)

end-reason	Description
<NOT PRESENT>	If not present, the flow ended normally (i.e., by TCP RST or FIN). Otherwise, the end-reason is one of the following strings below.
idle	Flow was expired by idle timeout. No packets were received for IDLE_TIMEOUT seconds and the flow was presumed closed.
active	Flow was expired by active timeout. The flow's duration was longer than ACTIVE_TIMEOUT seconds and the flow was flushed from the flow table.
eof	Flow was still active in the flow table at the end of the dumpfile or at yaf shutdown time; it was flushed as the flow table was cleared.
rsrc	Flow was prematurely flushed as idle because more than FLOW_TABLE_MAX flows were active in the flow table.
force	yaf forced a write of the flow, but the flow remained open. This is only seen if yaf operated with the --udp-uniflow flag, which exports each UDP packet as a flow record, but allows the flow to remain open until it closes naturally by idle and active timeouts.

Yaf – Fields with Uniflow Output

- All “Reverse” field values will be 0 in uniflow logs:
  - rpkt, roct, riflags, ruflags
- rtt field will also be 0 in uniflow logs

Lab 1001 – Flows/IPFIX

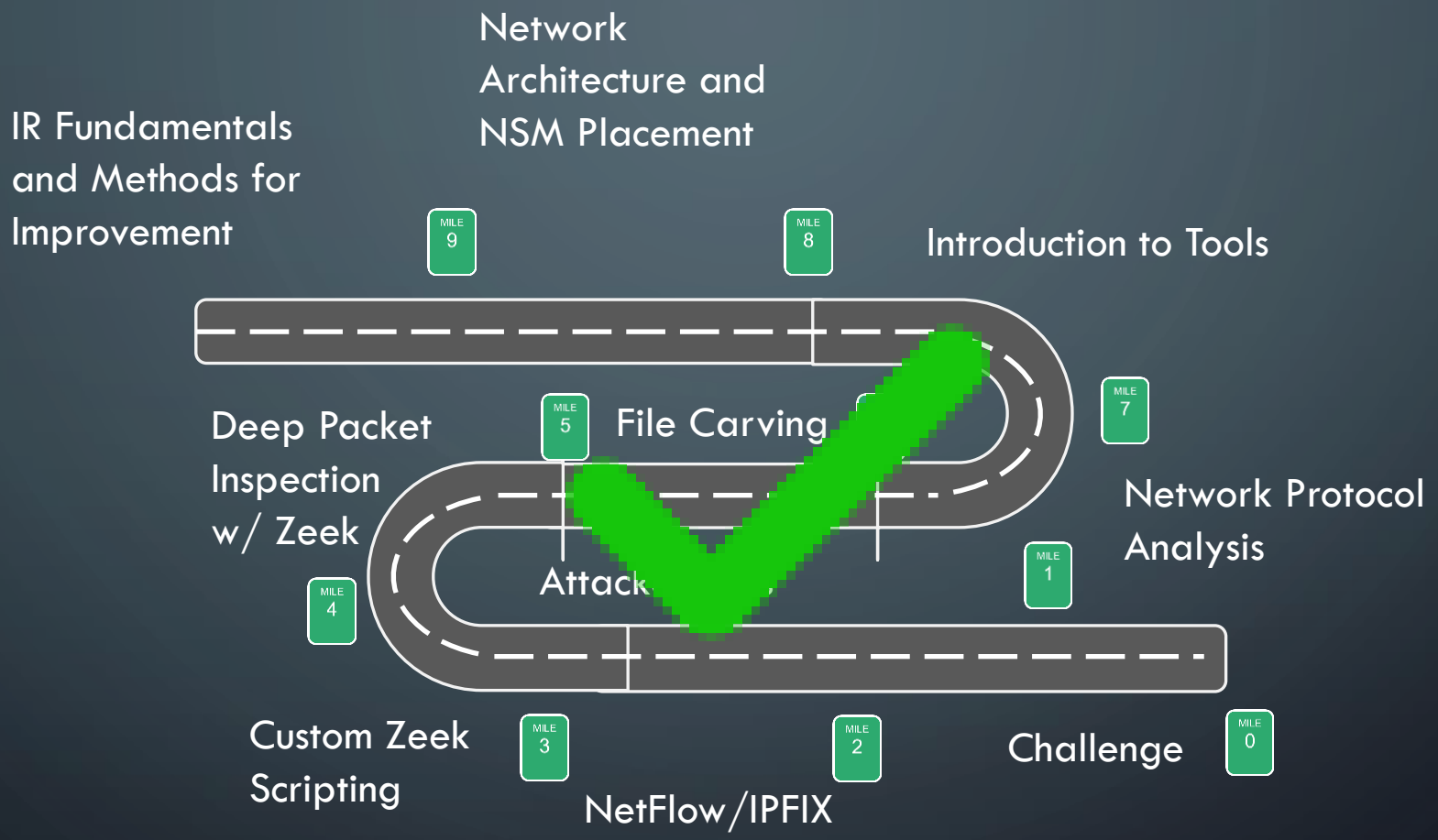
Checkpoint

Challenge

Get pcap here → https://ndfir.s3.amazonaws.com/lab-1010.zip

- What happened?
- Timeline of Key Events
- Should Doc be worried?
- IOCs?

Roadmap



<---------- event horizon ---------->

Thank You!

Special thanks to:

- YOU! Thank you so much for attending the course and wish you all well on your digital forensic ventures!
- Jason (The Hawk) and Shelby (The Kid) and all at Antisyphon!

Troy Wojewoda

0byte.offset@gmail.com

https://www.linkedin.com/in/troy-wojewoda-92387183