Exam subjects for Introduction to Incident Response

Below is the list of exam subjects. The subject is the headline, the bullets are keywords and are intended to describe what I consider as part of this subject, and not a complete list of the subject matter.

The exam will consist of:

- Selecting a subject from the list below - random draw using random.org
- Up to 10 minutes the student will present from prepared slide show
- Dialogue up to 15minutes questions

Total time 30minutes

Hints

Do NOT try to go through everything within 10 minutes
Keywords added are not expected to be used all within 10 minutes, but are example items that fit into this subject.

So a presentation from you could include 2-3-4 bullet points from a subject.

Feel free to include tools and references to tools throughout!

Subjects

1. Overview of Incident Response

- Why do we need Incident Response
- A few threats and context
- Definitions of Incident Response, Computer Forensics other main terminology
- Main resources we have used, IDIR book, NIST, other books

2. Cyber Attack Phases and IR

Main processes and methods within incident response

- intrusion kill chain, incident response cycle
- Overall description of how attacks happen, and how we deal with them
- Mitre ATT&CK framework can be used here

3. Incident Response Life Cycle

Detailed about what happens when we have identified an incident

- Go through the phases and explain as much as possible within 10minutes
- Use NIST SP800-61r2 figure 3-1, IDIR or other books or references as you wish
- You can also use the F3EAD process
- You can even present overview and compare instead

4. Order of Volatility and Tools

Explain the concept of Order of Volatility (OOV) from Forensics Discovery, Farmer Venema 2004

- List example tools, explain how they fit with volatility
- Why do we run memory tools first, and can wait with disk and storage analysis
- Live Response vs cold images and files with data
- Feel free to mention tools used for performing investigations according to the OOV

5. Evidence and IoCs

Anything related to facts we find and use

- Definitions of IoCs, examples of IoCs
- Domains, DNS, Passive DNS,
- File related, Hash values, IP addresses
- Enrichment and metadata related to facts
- Processing of facts, where do we find them
- Ideas Whois, RIPE Stat, RIPE delegated list of IP prefixes etc.
- Logging can also be used here

6. Tools we have used during the course

Take your favourite tool(s), maximum 2-3 tools we have used in classe, create screenshots,
Walk us through the process, what it provides, how the tool helps,
what is the output, why is this a good idea to use -- explain the tool, do not just include the description from their main web page

- Brim, tcpdump, wireshark, Packetbeat
- Sysinternals
- Zeek, Suricata
- Volatility framework
- Loki IOC and YARA scanner
- MISP Project
  … anything we mentioned in class or you tried during exercises is OK

Beware you CAN do demos, but if something goes wrong … better
to have a video without sound and present IMHO

7. How to establish an Incident Response Capability

- What are the steps to create this capability in an organisation
- Use input from NIST document and IDIR book also provides detailed information
- Also the exercise from March 30 may help
- Select the parts of this which interest you the most, can be organizational, technical or a mix
- Outline steps which you would propose to a CEO when you got hired as CISO

8. Vulnerability Cases

Ideas
a) Take a known vulnerability, like Log4Shell

- Go through how it works
- what it does

- what are prerequsites etc.
- What are some IoCs, signs of intrusion with this
- Focus on how this relates to Incident Response, how would an organisation react

OR

b) What preperative steps could help

- Configuration Management Database (CMDB)
- How would architecture changes reduce likelihood or prevent this from happening
- How can organisations learn from cases in other organisations

OR

c) Budgets and incident response

Talk about steps from the incident response life cycle and how it relates to cost
-- usually it is MUCH more efficient to spend a little on preparation, to shorten incidents