



Advanced Cybersecurity Essentials Workshop

Dr. Amin Hasbini

Previous labs/Homework

Lab/homework

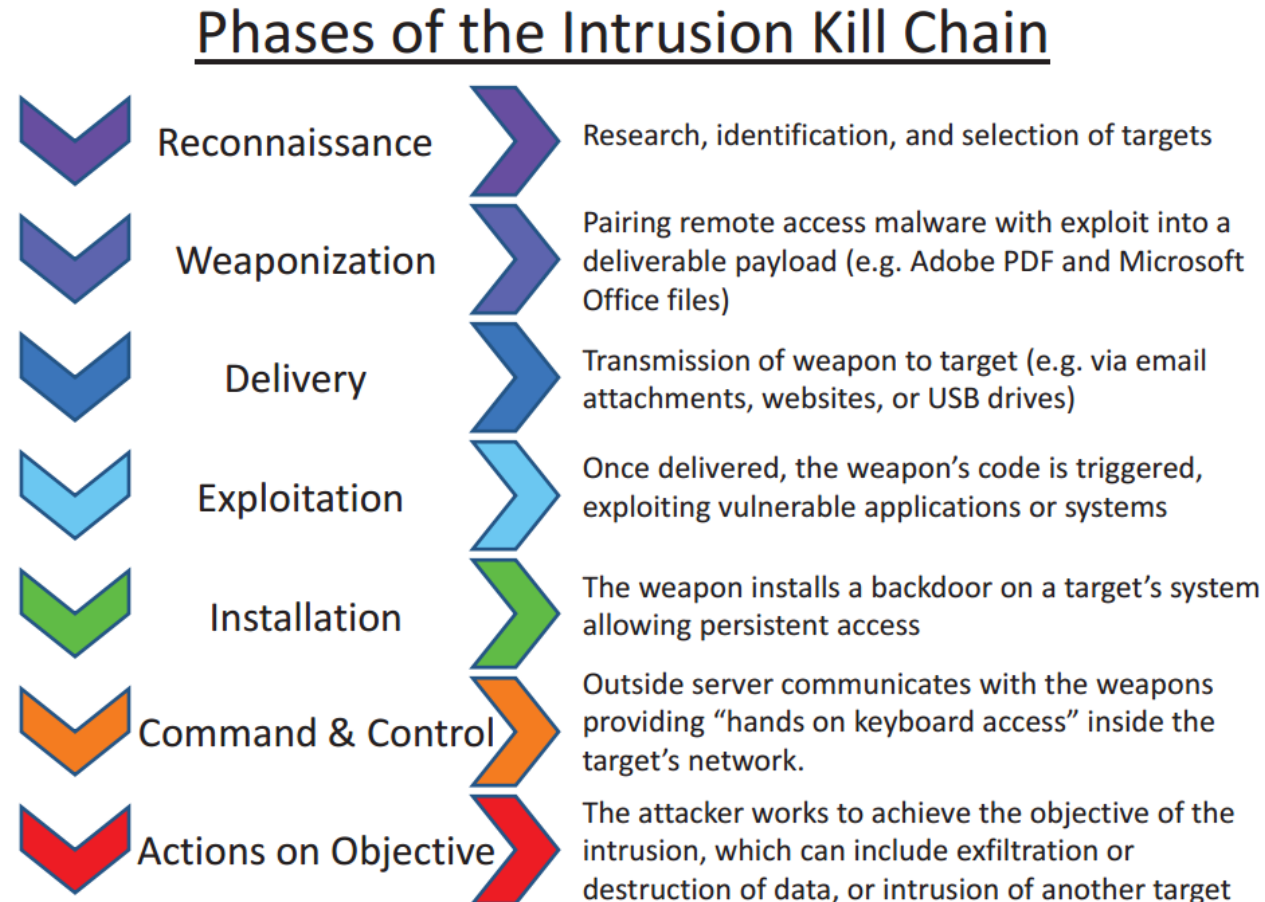
- Exercise on linux Ubuntu VM 20min: install nmap and run a quick port scan on your personal LAN network/gateway IP
- Exercise on linux Ubuntu VM: install Nikto and scan vulnerable VM
- Exercise on Kali linux: what exploitation attacks can you execute on vulnerable VM?
 - Information disclosure?
 - Misconfigurations?
 - Exploitation with Metasploit?
 - SQL injection?
- Research: what is Turla APT? earliest traces? List of campaigns? (10min)

Hints

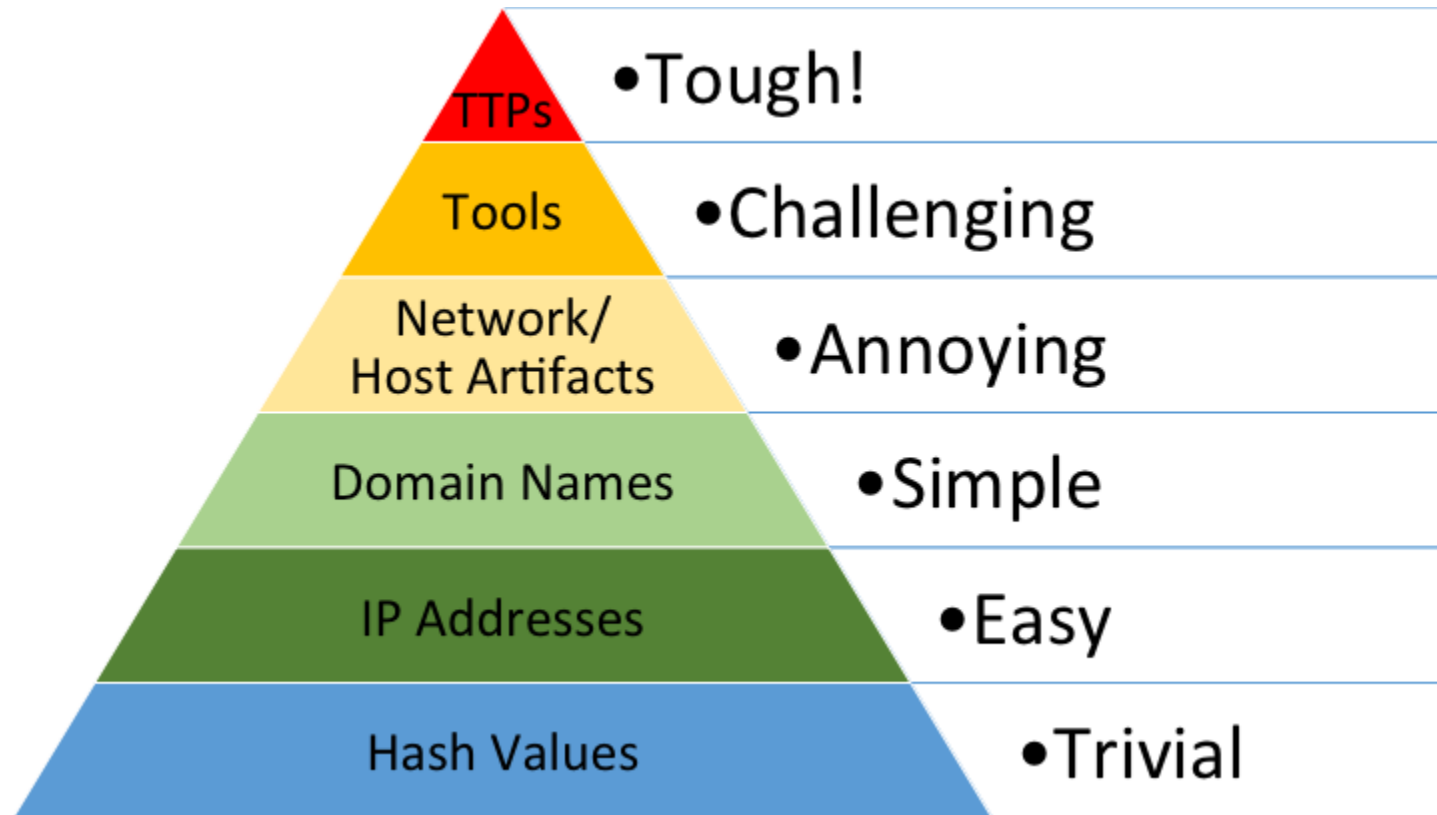
- Mutillidae for SQL injection
- You need to repair database access under `/var/www/mutillidae/config.inc`

Module 3 digital forensics and incident response

The intrusion kill chain



DFIR pyramid of pain



TTPs



Procedures

How the technique was carried out.
For example, the attacker used
`procdump -ma lsass.exe lsass_dump`

Techniques

Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics

Tactics represent the strategic goal of the adversary. For example, TA006 - Credential Access

MITRE ATT&CK (attack.mitre.org)

- Adversary analysis and profiling framework/platform
 - Techniques <https://attack.mitre.org/techniques/enterprise/>
 - Tactics <https://attack.mitre.org/tactics/enterprise/>
 - Groups <https://attack.mitre.org/groups/>
 - Software <https://attack.mitre.org/software/>
 - Data sources <https://attack.mitre.org/datasources/>
 - Matrices <https://attack.mitre.org/matrices/enterprise/>

DFIR process

DFIR

- When is it invoked?
- What does it invoke



GDPR Data Breach Notice Letter

My Company
Additional Information
Street, Number
City, Region
Country

Customer Name,

At My Company, we respect the privacy of your personal data. We are writing to let you know about a data security incident that involves the personal information you have with us.

On Jan 01, 2019, we have discovered a data breach in our systems. The data accessed may have included the following types of personal information:

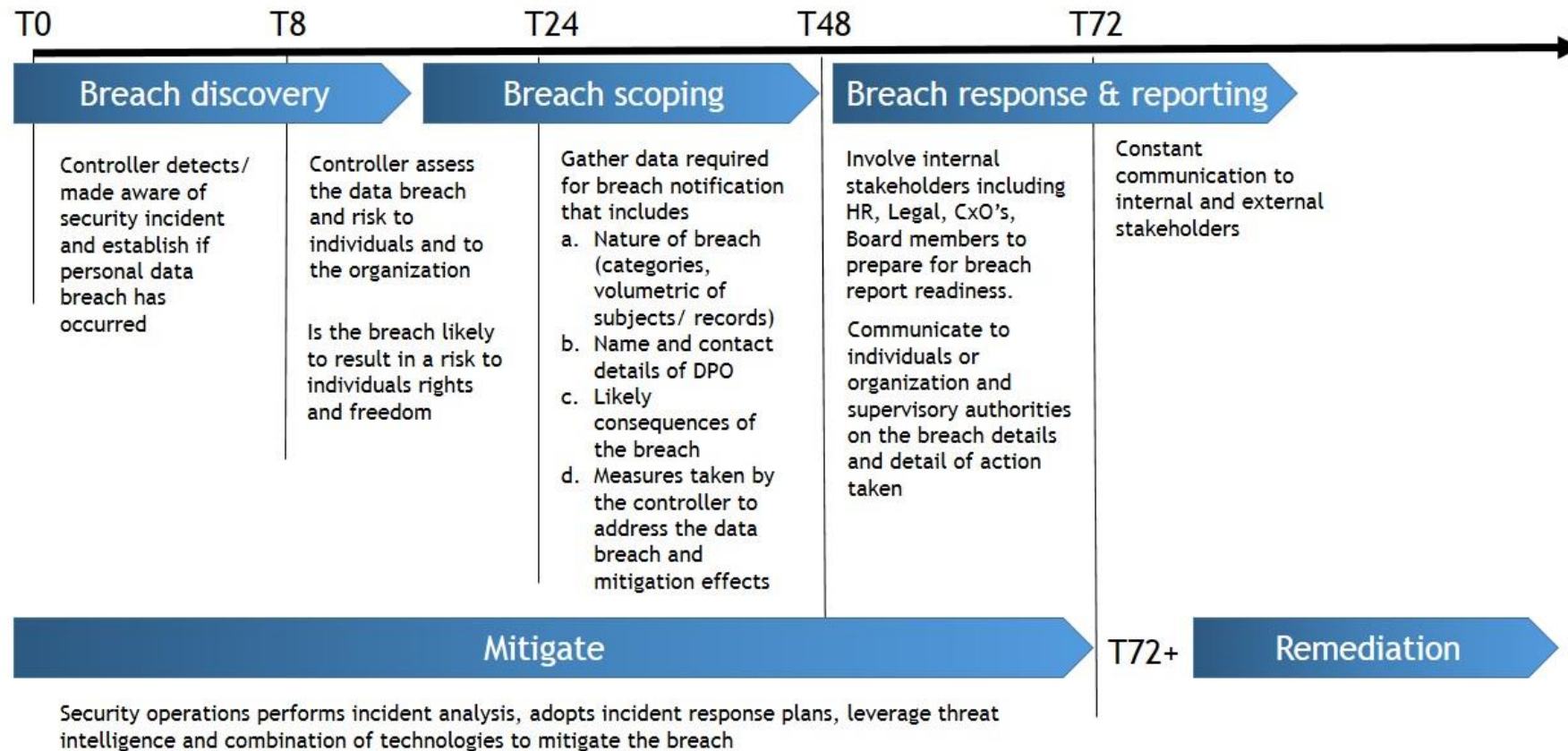
- Identify types of personal information breached: Email, First and Last Name

To the best of our knowledge, the data accessed did not include any:

- Identify types of personal information not breached: Shipping Address

We deeply regret that this incident occurred. We are conducting a review of the affected records and of all our computer systems. We will notify you if there are any significant developments.

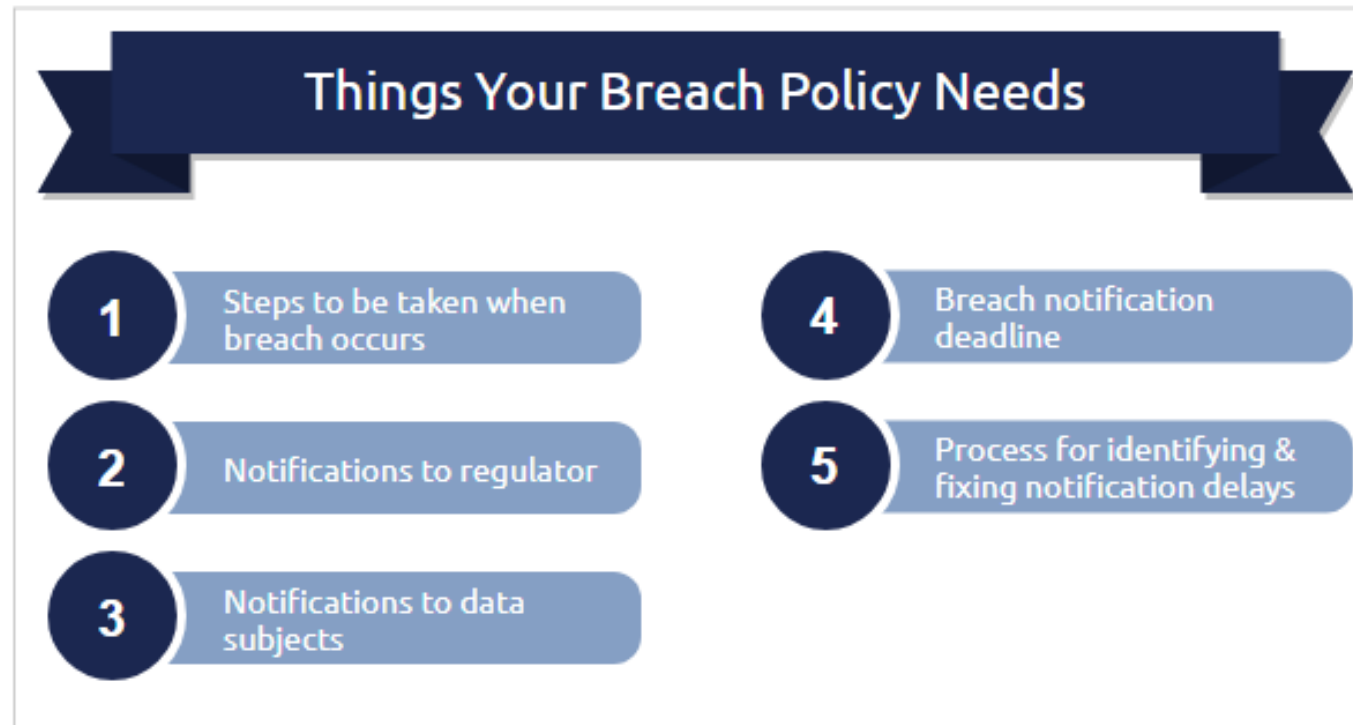
Breach notification process e.g. 72hours



DFIR role

- Compromise assessment/confirmation
- Incident impact
- Incident cause
- Evidence collection

The breach notification policy



<https://www.epiuselabs.com/data-security/gdpr-and-popia-data-breach>

The incident response plan

Section	Description
1 Introduction	• Purpose of response plan, initiation guidelines, and how to use the plan • Plan contents and scope of use
2 How to use the incident-response plan	• Explanation of the different levels of incident response and escalation points • Description of how to use the document for each part of the process
3 Event handling	• Event types, guidelines for categorization, and suggested actions
4 Incident topology	• Incident types • Affected information assets
5 Incident-response team and war room	• Team responsible for incident response
6 Setup of the war room	• Structure of working groups that are part of the war-room/critical-decision rights and responsibilities
7 Response plans	• Plans for each incident type • Plans for each information-asset type • Checklists of key processes, actions, and notifications to be triggered in the event of a cyberattack, categorized by both incident and asset type
8 Post-incident procedures	• Post-incident procedures and documentation of post-incident learning and codification: — Documenting incident details and response actions — Collecting lessons learned from incident response — Updating plan to improve future responses

DFIR process

- Acquisition
- Analysis
- Reporting

DFIR - Acquisition

- Disk images (dd, FTK imager...)
- Memory images (mdd, notmyfault...)
- Application data



A write blocker

DFIR - Analysis

- Disk creation and analysis: OSForensics, FTK, SleuthKit, autopsy, ProDiscover Basic, Volatility...
- Paid LEA tools (Cellebrite, Greykey, Magnet axiom...)
- The Kali Linux or the SANS SIFT VM appliance
- Linux systems analysis: CAINE
- Registry analysis: registry recon
- Network analysis: Wireshark

Disk analysis – data sources

- Physical drive (IDE/SATA/SCSI)
- Logical drive
- Image file
- Folder/files

Memory analysis

- Processes
- Threads
- Connections
- Last commands
- Registry artifacts

Application data

- Logs (operations, updates, access, AAAA)
- Files integrity checks

DFIR - Reporting

- Executive summary
- Technical analysis
- TTPs
- Victimology / attack scope
- Impact on business operations
- Attribution, correlation, similarities
- Recommendations
- Conclusion

DFIR - chain of custody

- Tracking the movement of evidence from collection, safeguarding and analysis
- Evidence must be kept safe:
 - Admissible in court
 - Authentic
 - Complete
 - Reliable
 - Believable

DFIR - skillset

- File forensics
- Memory forensics
- Network forensics
- Malware analysis
- Log analysis
- Software development
- Communication skills / teamwork

Top DFIR standard references

- The National Institute of Standards and Technology (NIST) incident response framework
- ISO/IEC 27035

MSSPs – Managed security service providers

- 24x7 correlated log monitoring and management
- 24x7 threat mitigation
- Firewalls
- Intrusion prevention
- Vulnerability scanning
- Content filtering
- Encryption
- Endpoint security
- Host intrusion prevention security (HIPS)
- Secure mobile device managemtn
- Phishing detection ad takedowns

China Hacked Eight Major MSPs, Technology Service Providers: Report

Hackers working for China broke into the networks of eight major MSPs & technology services providers to penetrate end-customer systems, a report says.

by Joe Panettieri • Jun 26, 2019

Hackers working for China's Ministry of State Security broke into networks of eight major MSPs and technology services providers in an effort to steal commercial secrets from the MSPs' customers, [a Reuters report alleges](#).

The so-called Cloud Hopper attacks (aka [Island Hopper attacks](#)), according to Reuters, penetrated:

- Computer Sciences Corp. (now DXC)
- [Dimension Data](#)
- [DXC Technology](#). (HPE's spun-off services arm)
- [HP Enterprise](#)
- [IBM](#)
- [Fujitsu](#)
- [NTT Data](#)

This document is TLP RED



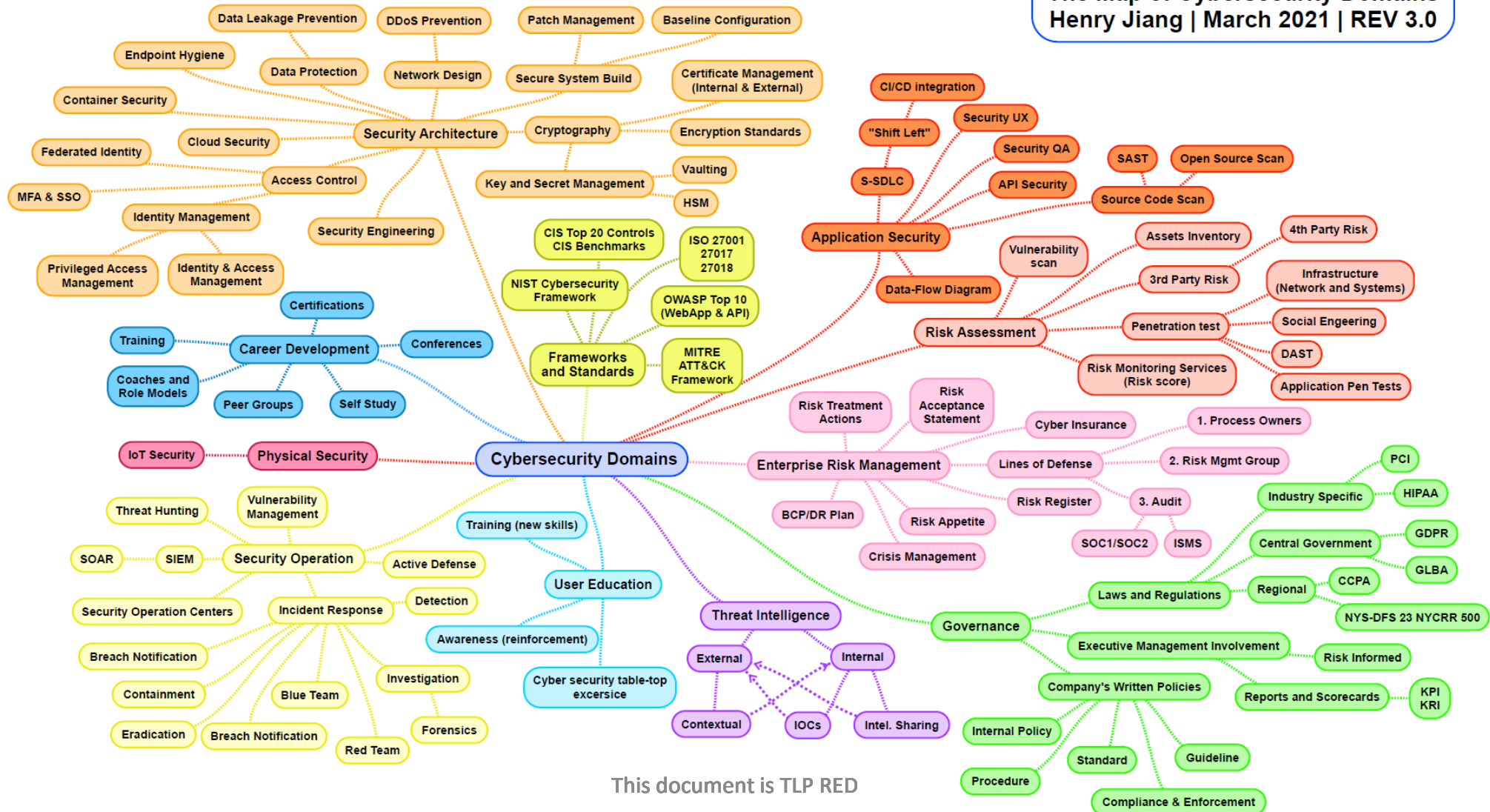
End of Module 3 digital forensics and incident response

Dr. Amin Hasbini

Future thoughts and career analysis

The cybersecurity domains map

The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.0



This document is TLP RED

[illegible]

31

2022 Barclay Simpson Salary & Recruitment Trends Guide

<https://www.barclaysimpson.com/resources/BSA%20Salary%20Guide%20v7.pdf>

Labs

9. Analyze PCAP capture using wireshark (easy-15min)
 - <https://www.wireshark.org/download.html>
10. Create a memorydump using Notmyfault on Win VM from command line (easy-15min)
 - <https://docs.microsoft.com/en-us/sysinternals/downloads/notmyfault>
11. Analyze http log using the following commands and find suspicious domain on Kali (or Ubuntu) (Intermediate-25min)
 - Commands: cat, cut, less, sort, uniq, grep, >, >>
 - Create bash script to analyze http log

<https://drive.google.com/drive/folders/1Y6myMLpNqveqNnUL7hOvjhKB9OvEewWV?usp=sharing>

Labs 2/2

12. Disk forensics using autopsy, analyze a USB image collected from a crime scene (easy to intermediate-25min)

- <https://www.autopsy.com/download/>
- What is the disk format of Charlie's USB? How many PDFs can be found on Charlie's USB?
- What other useful evidence can be found on Charlie's USB regarding project2400?

13. Memory forensics using volatility, analyze a memory dump collected from a cridex fraud victim (intermediate to hard-40min)

- <https://www.volatilityfoundation.org/releases> (standalone version best)

<https://drive.google.com/drive/folders/1Y6myMLpNqveqNnUL7hOvjhKB9OvEewWV?usp=sharing>