Best Practices for Documentation

SoftUni Team

Technical Trainers

Software University

SoftUni

Software University

https://softuni.bg

Have a Questions?

Software University

sli.do

#Cyber_Security

Table of Contents

Why Taking Notes is Important?

Taking Notes is a Must!

Software University

- When conducting **penetration testing**, or other security operations, taking notes is essential for not getting lost and getting a good report
- Imagine a real engagement, only from your **reconnaissance** process, you can generate a tons amount of notes
- Imagine finding a vulnerability and exploiting it?
- When doing penetration **testing**, you are responsible for your actions
- The way to prove your actions are your notes and screenshots

How to Take Notes Efficiently?

In the Scope of the Course, we Will Use Obsidian

Software University

- Obsidian is highly customizable local note taking application
- It has cloud sync but we will stick to local files only
- Feel free to **customize obsidian** as your willing
- It has a huge amount of methods and plugins, helping you getting smoother experience
- Obsidian config is stored per project
- That means if you were to **generate new project** you are with the defaults again

In the Scope of the Course, we Will Use Obsidian

Software University

- To migrate your configuration, copy **.obsidian folder** from your previous project (when you configured obsidian) to your **current folder**
- My configuration is provided with the materials
- When migrating a configuration, if you were using community plugins, obsidian will ask if you want to allow them
- If you feel comfortable and trust me, click enable plugins haha

Note Taking Methodology

Software University

- There is no accepted or best practical way of taking notes. It is a good idea to play around a find a way that works for you
- Even though there is not a **methodology**, I need to explain a few really important things
- The main goal of taking notes is to know what, when and how
- For example, you found an **SQL injection**
- My best practice is to document with what payload you managed to find the vulnerability, how did you exploited it, and what did you get
- For all of these steps I would **inlucde request** / **response** from burp or sqlmap, as well as screenshots
- Start small but build up a **structure** for yourself!

Note Taking Methodology

- One of the best way of organizing your notes (**when doing pentest or red teaming operations**) is the following:

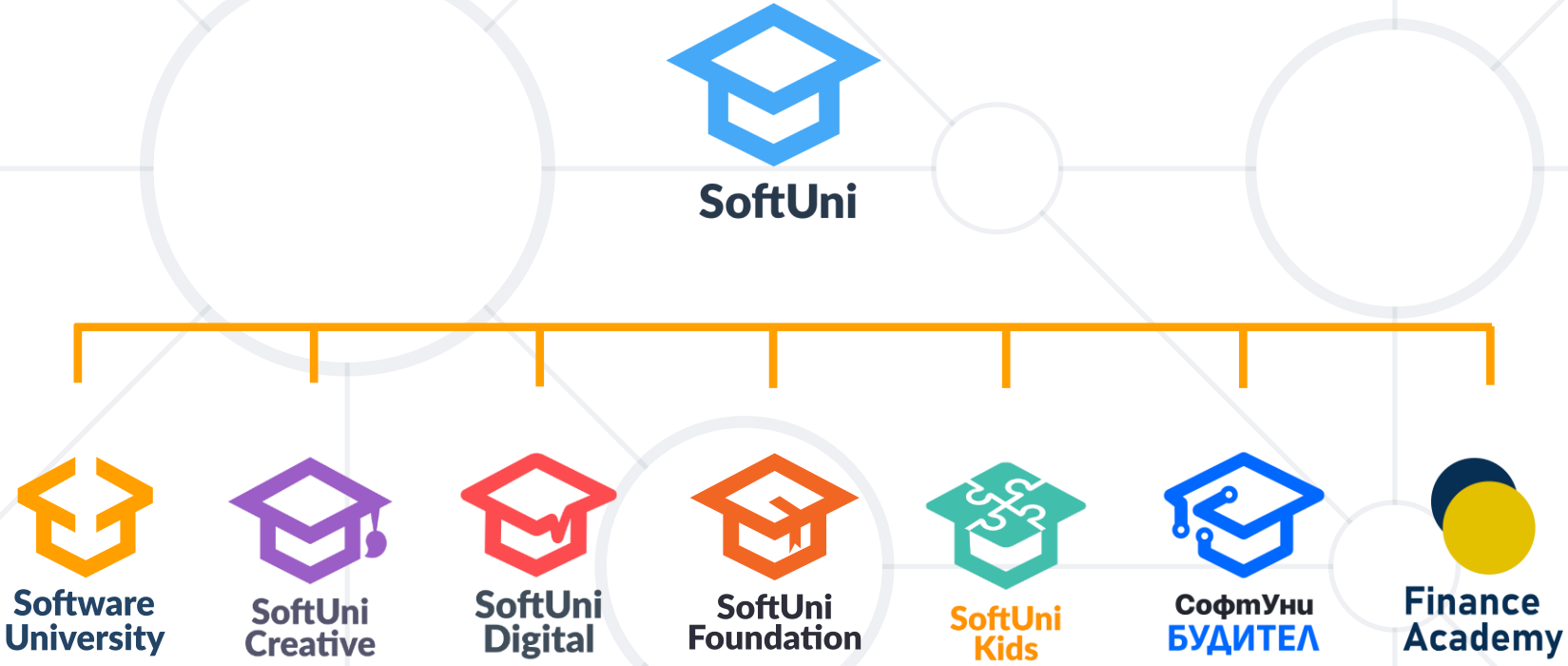
```
engagement_name
├── 0-admin
├── 1-osint
├── 2-recon
├── 3-targets
│   ├── domain_name
│   │   └── exfil
│   └── ip_hostname
│       └── exfil
├── 4-screenshots
│   └── YYYYMMDD_HHMM_IP_Description.png
├── 5-payloads
├── 6-logs
└── readme.md
```

- Let's demonstrate it!

Summary

- Taking notes is a **must**!
- Implement custom note taking methodology

Questions?



SoftUni Diamond Partners

Software University

SmartIT

Coca-Cola HBC Bulgaria

SUPER HOSTING .BG

createX

Postbank

Решения за твоето утре

DRAFT KINGS

THE CROWN IS YOURS

VIVACOM

AMBITIONED

INDEAVR

Serving the high achievers

PHAR VISION

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, about.softuni.bg
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity

License

- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**
- Unauthorized copy, reproduction or use is illegal
- © SoftUni – https://about.softuni.bg/
- © Software University – https://softuni.bg