# Notes on the Current version of the Deakin Detonator Tool Kit

Purpose:

So that I can better understand the GUI and have ideas for how I can contribute to this project

## Sections (By pages)

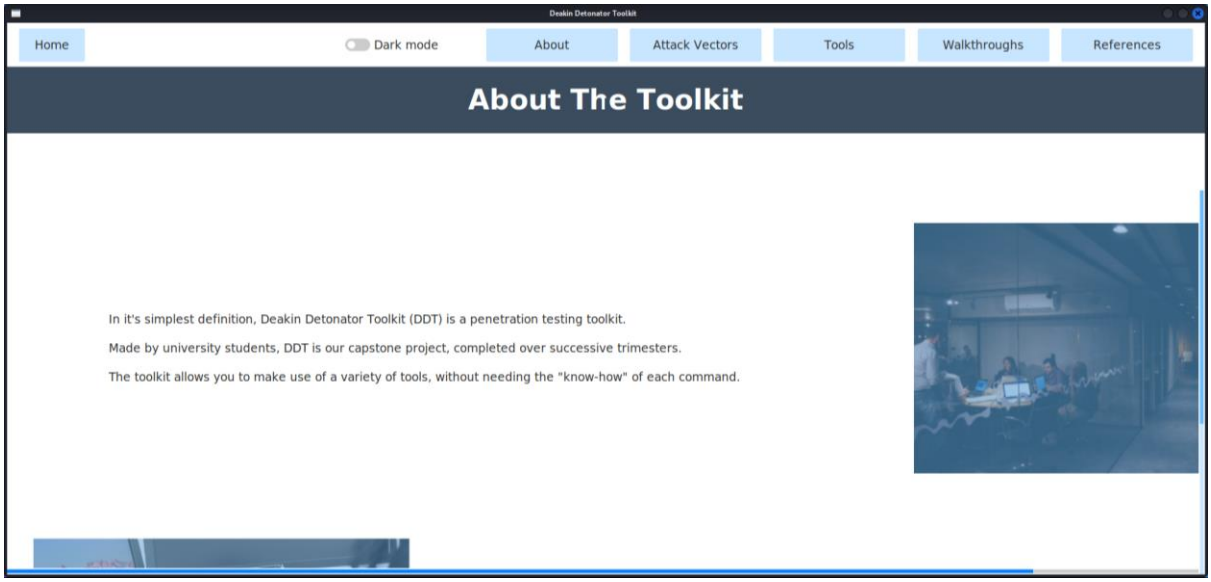
## Contents

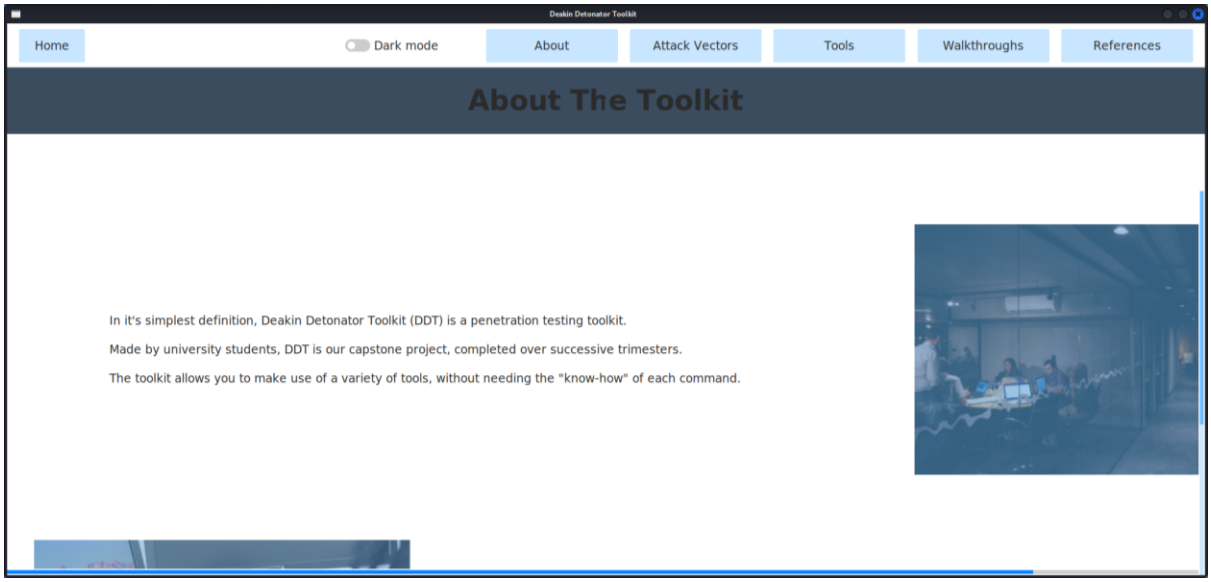
## Startup - Home Page

- No apparent bugs or issues with the Home Page.
- Proposed improvement of changing colours for the menu options so they are more symmetrical (colour order of 1,2,3,2,1 instead of 1,2,1,3,5)
- A potential change of the title.
- Could use a search bar and a logo.


## About Page

- The content of the page is bigger than the frame, so it requires a scroll bar and cuts off information oddly.
- Page scroll does not work with mouse scroll wheel and arrow keys. That can be changed.
- Photos have a heavy blue tinge looking like they have been selected by the mouse.
- Permanent thick white/grey bar at the top of the page cuts of information.
- Heading goes from white to grey with Dark Mode and stays grey when Dark Mode is turned off
- Heading is slightly obstructed by something (letter h)






## Attack Vectors Page

- Same scrollbar issues as the About page (not working with mouse scroll wheel and keyboard keys)
- Same white/grey bar at the top of the page
- Same heading colour and obstruction problem as the About Page after turning on Dark Mode once
- No titles or context for the page (For example: Attack Vector – Reverse TCP Shell, Author/Tool creator – Daniel Sacchetta, Information – Information Icon, Launch Tool – LAUNCH button).
- Information icons not responding.
- NFS Privilege escalation does not have a description (checked the code file, it was an empty fields)
- Same heading colour and obstruction problem after turning on Dark Mode once

### Reverse TCP Shell

- Only diagram explanation with no text explanation of the tool or what the steps are
- No way to get back to the explanation diagram after clicking a step on the side menu without going back to the Attack Vectors page
- Step1: Payload generator button is floating within the text
- Step1: No way to get back to the attack vector page with steps after clicking on the payload generator button without navigating back to the Attack Vectors page
- Step1: IP address is automatically set as a default and there's no way to change it without clicking no button and being prompted to another page. Look into adding a text field with a prefilled but editable value. Same thing with port number.
- Step1: Save payload file and generate payload are separate buttons on separate pages, work on merging both buttons' functions so that when a user creates the payload the file the payload is automatically loaded onto that file.
- Step1: After generating the payload, you're directed to generate a payload again and not Step2. There is no way to get to Step 2 without getting back to the Attack Vectors page.
- Step2: Floating button again.

- Step2: Button directs to another blank page with a single button (redundant)
- Step2: No back button
- Step2: Same suggestion for the default IP address and default port
- Step2: Needs a better way to know if you picked the 'Start Listening' button, current method is a colour change but that might not be clear enough.
- Step2: Either freezes the application completely on this listening scene or the application crashes.
- Step2: We need feedback if the connection doesn't happen so the screen and application don't get stuck on awaiting a connection.
- Needs a stop listening button or a time limit for waiting for a connection (on my tries I've had it loading for at least 30 minutes if it didn't already crash by then)
- Step2: Currently, the only way out of step 2 is to force close the application from the terminal (the close GUI button would not work) and restart it.

Terminal Error message:

- File "/usr/lib/python3/dist-packages/requests/adapters.py", line 516, in send raise ConnectionError(e, request=request) requests.exceptions.ConnectionError: HTTPConnectionPool(host='127.0.0.1', port=55553): Max retries exceeded with url: /api/ (Caused by NewConnectionError('<urllib3.connection.HTTPConnection object at 0x7fef603d09a0>: Failed to establish a new connection: [Errno 111] Connection refused'))

## Directory Traversal & IDOR

- Same problem with the diagram being presented with no text.
- Same problem with not seeing the diagram again after clicking a step
- Step1: Button is in correct place, but the text is too long for the button size (when screen is smaller than full size)
- Step1: Needs a note that the webpage must begin with HTTP or HTTPS
- Step1: Would be nice if clicking the Visit Homepage button automatically updated/set the homepage without needing the user to manually do it by pressing the set home page button
- Step 1: Application froze after auto scanning for directories and needed to be rebooted
- Step 2: Same exact tool as step 1 with no changes (redundant)

## Unpatched Vulnerabilities and Exploits

- Same problem with the diagram being presented with no text.
- Same problem with not seeing the diagram again after clicking a step
- Step1: No default or example IP address
- Step1: Could use an information button around speed meanings
- Step1: Cannot select text from text example. Maybe add copy text button.
- No real issues that I would tell with step 2 and 3 except that it could use a bit more information on what's going on.

## Web Application Attacks: Automated XSS and SQL injection attack

- ~~Same problem with the diagram being presented with no text.~~

- ~~Same problem with not seeing the diagram again after clicking a step~~
- Under maintenance

### NFS Privilege Escalation

- Blank landing page with no image or text.
- Same problem with not seeing the previous page again after clicking a step
- Same problem with not being able to copy commands
- Terminal execution so no further GUI problems

### Apache WebServer Exploit

- Same problem with the diagram being presented with no text.
- Same problem with not seeing the diagram again after clicking a step
- Step1: Same problem with floating button
- Step2: The python code cannot be found therefore the exploit can't be run

Terminal Error message:

- FileNotFoundError: [Errno 2] No such file or directory: './Tools'
- Exception in Tkinter callback
- Traceback (most recent call last):
- File "/usr/lib/python3.9/tkinter/__init__.py", line 1892, in __call__return self.func(*args)
- File "/home/kohas/Documents/PT-GUI/ATTACKVECTOR/attackvector8.py", line 42, in load_exploit os.chdir("./Tools")
- FileNotFoundError: [Errno 2] No such file or directory: './Tools'

### Authentication Bypass Attack

- Same problem with the diagram being presented with no text.
- Same problem with not seeing the diagram again after clicking a step
- Step1: Hint button is floating and covering the text
- Step1: Could use a button to open Command Prompt like the Terminal Button
- Step2: Terminal launch button is floating and covering text
- Same issues with not being able to copy text

## Tools Page

- Same scrollbar issues as the other pages (not working with mouse scroll wheel and keyboard keys)
- Different header to the rest of the toolkit
- Doesn't have the white/grey bar (good)
- Page information is not aligned in the middle of the page like the rest of the application pages.

## Walkthroughs Page

- Same scrollbar issues as the other pages (not working with mouse scroll wheel and keyboard keys)
- Same white/grey bar at the top of the page
- Same heading colour and obstruction problem as the other pages after turning on Dark Mode once
- Instructions for the Video Player are in the heading
- Video Player needs a status bar and icons for play/pause, fast forward 10s, rewind 10s, volume control, and speed control
- When you exit out of the video, the video's audio continues for a few seconds afterwards

## References Page

- Same scrollbar issues as the About page (not working with mouse scroll wheel and keyboard keys)
- Same white/grey bar at the top of the page
- Same heading colour and obstruction problem as the other pages after turning on Dark Mode once
- Could use a contents table with section links to find references faster
- Attack vectors are numbered and without specific titles
- Links can only be copied, not directed to
- Could use collapsible section headings like done on the tools page