U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND
ANALYSIS CENTER (DAC)

Emerging Results Brief (ERB) Generator

Salvador Melendez, Ph.D.

Computer Engineer

DEVCOM DAC

28 Apr 2020

BACKGROUND

Identified Issue:

- When attending cyber assessments, the team lead must present the *Emerging Results Brief* (ERB) to the customers/stakeholders.
- This is usually done by creating a PowerPoint slide deck with all the findings gathered by the other cyber analysts throughout the week.
- Usually the team lead has to spend a good amount of time the day before the final presentation; putting slides together for every finding: 1) affected hosts, 2) posture, 3) issues, 4) mitigation strategies, and 5) screenshots as evidence.

Proposed Solution:

- A Python Script with a Graphical User Interface (GUI) in the front end and some methods in the backend. This will save a lot of time and effort to the team lead preparing the ERB.

ERB-GEN SYSTEM

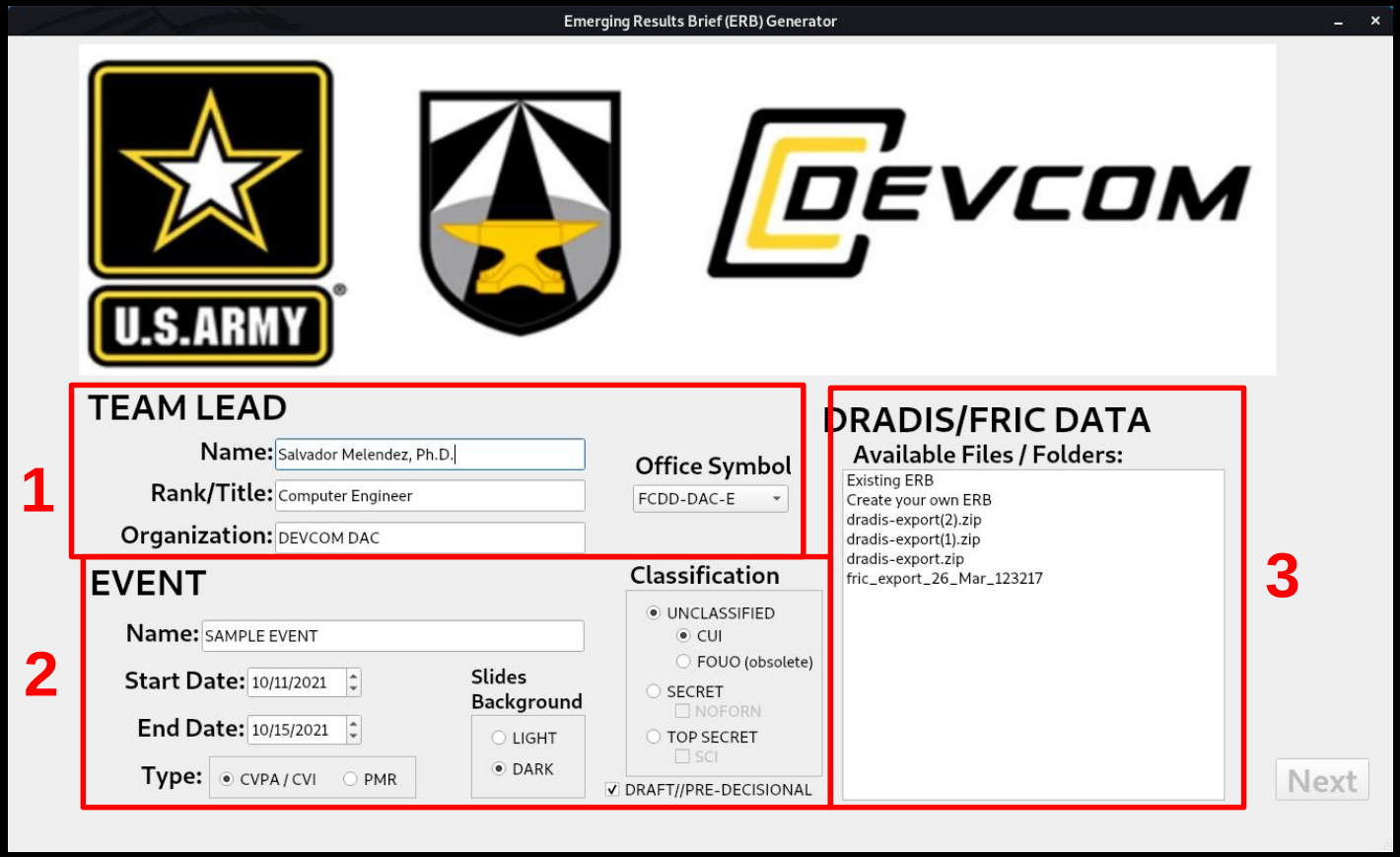
Dradis Data
or
FRIC Data
+
Python Script
=
PowerPoint

PROCESS:

1) Data from Dradis or FRIC is exported into your "*Desktop*"
2) Dradis or FRIC data is ingested into the Python Script
3) Using the GUI, the team lead will be able to:
   - Input the team lead's information
   - Input the event's information
   - Select the Dradis zip file or the FRIC folder with the correct data
   - Edit each of the findings (e.g. name, hosts, issues, posture, mitigation)
   - Re-arrange the findings in a different order
   - Add and/or delete any findings (if needed)
   - Select, re-arrange, delete the screenshots for each of the findings
4) Produce a PowerPoint Presentation

ERB-GEN GUI

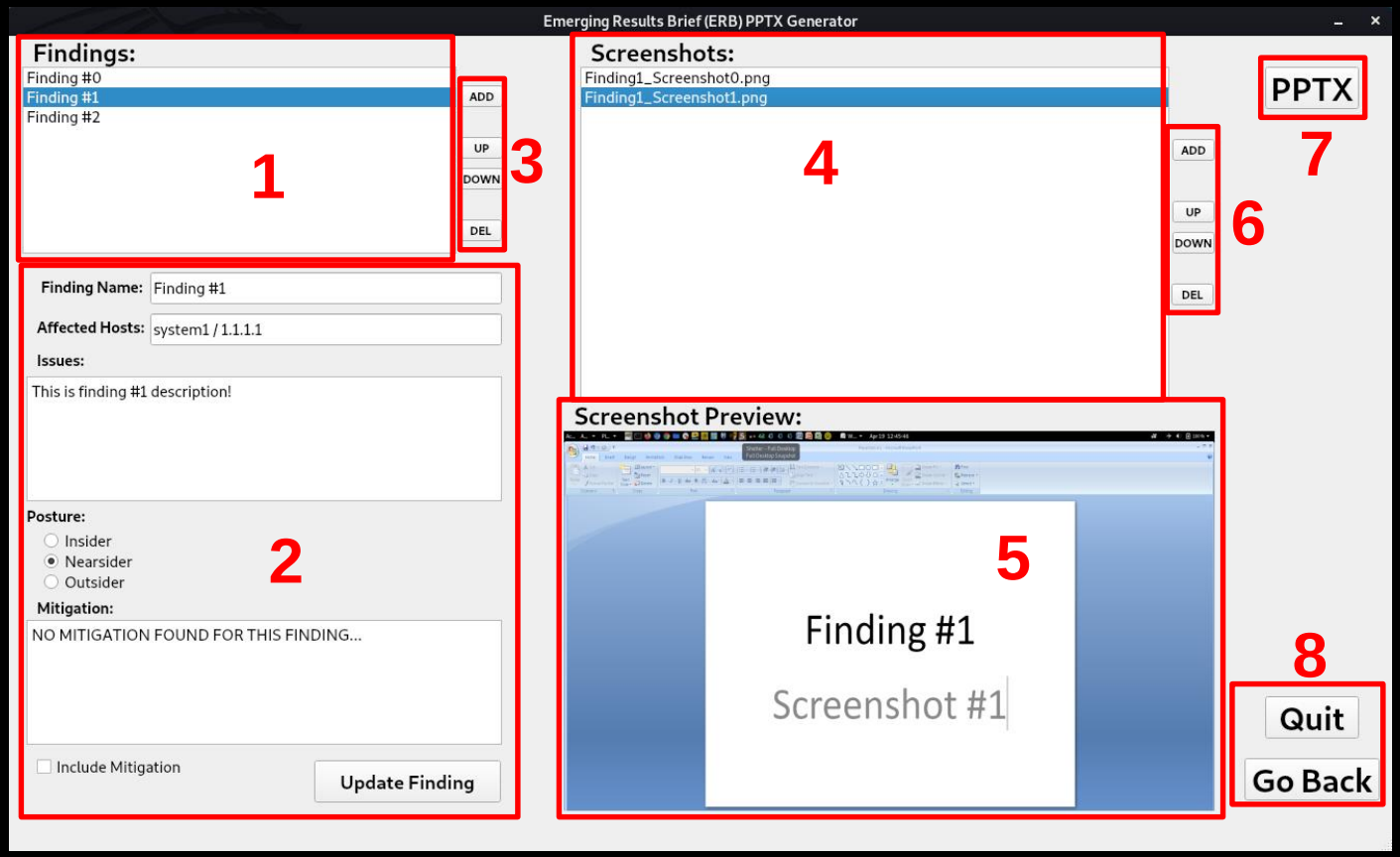
Page #1



1 – Team Lead's Information: name, title, organization, office symbol
2 – Event's Information: name, start/end dates, type, slides background, classification
3 – Dradis/FRIC Data: available files/folders with exported Dradis/FRIC data

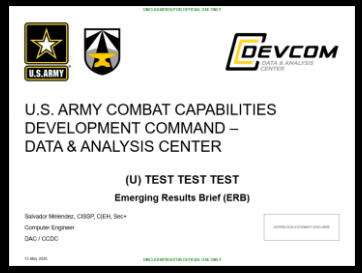
ERB-GEN GUI

Page #2

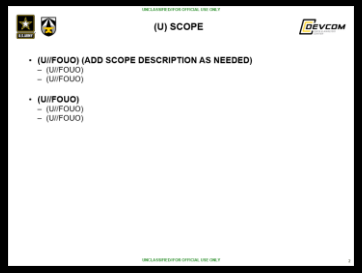


1 – Findings List
2 – Finding's Fields
3 – "Add/Up/Down/Delete" buttons to re-arrange the findings
4 – Screenshots List
5 – Screenshot Preview
6 – "Add/Up/Down/Delete" buttons to re-arrange the screenshots
7 – "PPTX" button to create the PowerPoint File
8 – "Quit" / "Go Back" buttons

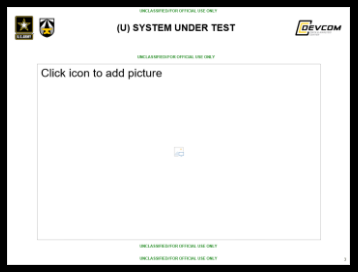
POWERPOINT SLIDE DECK



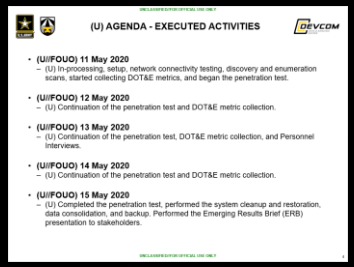
Cover Page



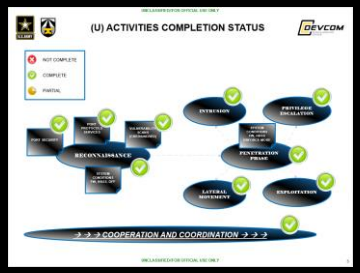
Scope



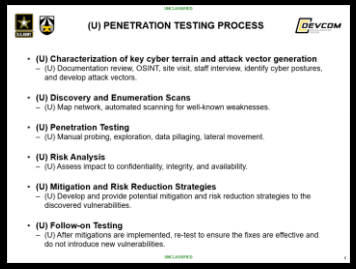
System Under Test



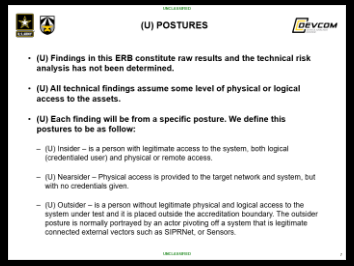
Agenda



Completion Status



PenTest Process



Postures

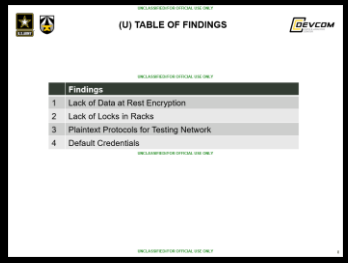
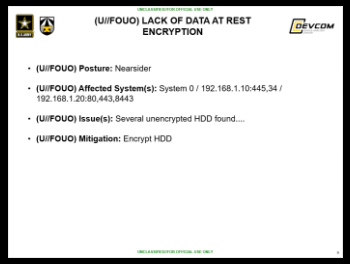
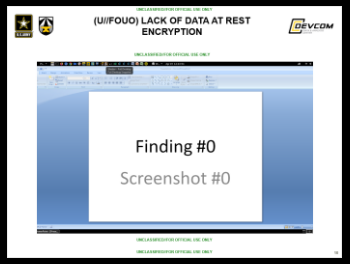


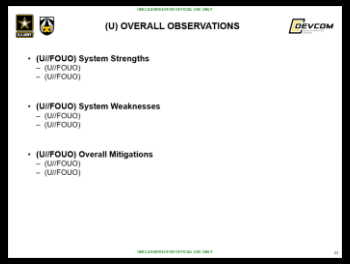
Table of Findings



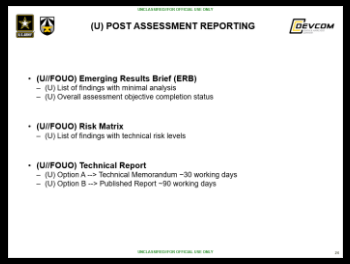
Finding's Info (Hots, Issues, Posture, Mitigation)



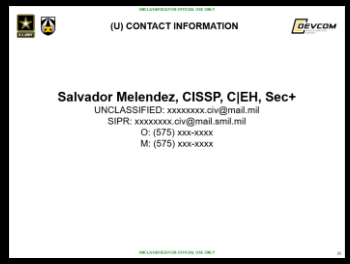
Screenshots



Overall Observations



Post Assessment Reporting



Contact Information

TUTORIAL

INSTRUCTIONS ON HOW TO USE THE ERB GENERATOR:

1) Unzip the file "erb-gen_v3.3.zip" into your "Desktop".
   You should have a folder named "erb-gen" with several files.

2) Export your Dradis findings into your "Desktop".
   It should be a zip file called "dradis-export".
   Do NOT rename it and do NOT unzip it.

3) Open a Terminal window and navigate to the "erb-gen" folder:
   cd /root/Desktop/erb-gen

4) Run the tool with this command --> python3 erb-gen.py

5) Use the GUI to generate your PPTX file; it should be self-explanatory.

6) When you hit the "PPTX" button, you should have your ERB in your "Desktop".

7) Open the Windows VM and use Microsoft Office PowerPoint to open the ERB file (recommended).

8) Complete the slides that are specific to your event.

CONTACT INFORMATION

Salvador Melendez, Ph.D.
UNCLASSIFIED email: salvador.melendez3.civ@army.mil