



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

## Emerging Results Brief (ERB) Generator

Salvador Melendez, Ph.D.

Computer Engineer

DEVCOM DAC



# 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.

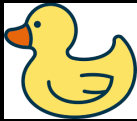


# ERB-GEN SYSTEM



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

Emerging Results Brief (ERB) Generator

**TEAM LEAD**

Name:

Rank/Title:

Organization:

Office Symbol:

**EVENT**

Name:

Start Date:

End Date:

Type: ☒ CVPA / CVI ☐ PMR

Slides Background: ☐ LIGHT ☒ DARK

Classification: ☒ UNCLASSIFIED ☒ CUI ☐ FOUO (obsolete) ☐ SECRET ☐ NOFORN ☐ TOP SECRET ☐ SCI

☒ DRAFT//PRE-DECISIONAL

**DRADIS/FRIC DATA**

Available Files / Folders:

Existing ERB

Create your own ERB

dradis-export(2).zip

dradis-export(1).zip

dradis-export.zip

fric\_export\_26\_Mar\_123217

Next

- 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

The screenshot displays the 'Emerging Results Brief (ERB) PPTX Generator' interface. It is divided into several sections:

- Findings:** A list containing 'Finding #0', 'Finding #1' (highlighted), and 'Finding #2'. To its right are buttons for 'ADD', 'UP', 'DOWN', and 'DEL'.
- Findings Fields:** A section for 'Finding #1' with fields for 'Finding Name', 'Affected Hosts' (containing 'system1 / 1.1.1.1'), 'Issues' (containing 'This is finding #1 description!'), 'Posture' (with radio buttons for 'Insider', 'Nearsider' (selected), and 'Outsider'), and 'Mitigation' (containing 'NO MITIGATION FOUND FOR THIS FINDING...'). It also includes an 'Include Mitigation' checkbox and an 'Update Finding' button.
- Screenshots:** A list containing 'Finding1\_Screenshot0.png' and 'Finding1\_Screenshot1.png'. To its right are buttons for 'ADD', 'UP', 'DOWN', and 'DEL'.
- Screenshot Preview:** A preview window showing a slide titled 'Finding #1' with the text 'Screenshot #1'.
- Buttons:** A 'PPTX' button at the top right and a 'Quit' / 'Go Back' button at the bottom right.

Numbered callouts (1-8) are placed over the interface elements as described in the legend.

- 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



**U.S. ARMY COMBAT CAPABILITIES  
DEVELOPMENT COMMAND –  
DATA & ANALYSIS CENTER**

**(U) TEST TEST TEST  
Emerging Results Brief (ERB)**

Salvador Melendez, CISSP, CJEH, Sec+  
Computer Engineer  
DAC / CDC

11 May 2020

**Cover Page**

**(U) SCOPE**

- (U//FOUO) (ADD SCOPE DESCRIPTION AS NEEDED)
  - (U//FOUO)
  - (U//FOUO)
- (U//FOUO)
  - (U//FOUO)
  - (U//FOUO)

**Scope**

**(U) SYSTEM UNDER TEST**

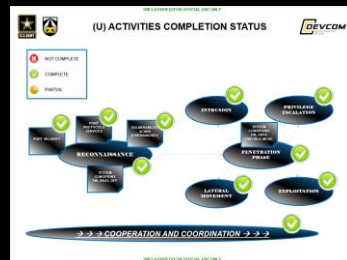
Click icon to add picture

**System Under Test**

**(U) AGENDA - EXECUTED ACTIVITIES**

- (U//FOUO) 11 May 2020
  - (U) In-processing, setup, network connectivity testing, discovery and enumeration scans, started collecting DOT&E metrics, and began the penetration test.
- (U//FOUO) 12 May 2020
  - (U) Continuation of the penetration test and DOT&E metric collection.
- (U//FOUO) 13 May 2020
  - (U) Continuation of the penetration test, DOT&E metric collection, and Personnel Interviews.
- (U//FOUO) 14 May 2020
  - (U) Continuation of the penetration test and DOT&E metric collection.
- (U//FOUO) 15 May 2020
  - (U) Completed the penetration test, performed the system cleanup and restoration, data consolidation, and backup. Performed the Emerging Results Brief (ERB) presentation to stakeholders.

**Agenda**



**Completion Status**

**(U) PENETRATION TESTING PROCESS**

- (U) Characterization of key cyber terrain and attack vector generation
  - (U) Documentation review, OSINT, site visit, staff interview, identify cyber postures, and develop attack vectors.
- (U) Discovery and Enumeration Scans
  - (U) Map network, automated scanning for well-known weaknesses.
- (U) Penetration Testing
  - (U) Manual probing, exploration, data pilging, lateral movement.
- (U) Risk Analysis
  - (U) Assess impact to confidentiality, integrity, and availability.
- (U) Mitigation and Risk Reduction Strategies
  - (U) Develop and provide potential mitigation and risk reduction strategies to the discovered vulnerabilities.
- (U) Follow-on Testing
  - (U) After mitigations are implemented, re-test to ensure the fixes are effective and do not introduce new vulnerabilities.

**PenTest Process**

**(U) POSTURES**

- (U) Findings in this ERB constitute raw results and the technical risk analysis has not been determined.
- (U) All technical findings assume some level of physical or logical access to the assets.
- (U) Each finding will be from a specific posture. We define this postures to be as follows:
  - (U) Insider – is a person with legitimate access to the system, both logical (predefined user) and physical or remote access.
  - (U) Nearsider – Physical access is provided to the target network and system, but with no credentials given.
  - (U) Outsider – is a person without legitimate physical and logical access to the system under test and it is placed outside the accreditation boundary. The outsider posture is normally portrayed by an actor pivoting off a system that is legitimate connected external vectors such as SIPRNet, or Sensors.

**Postures**

**(U) TABLE OF FINDINGS**

Findings
1. Lack of Data at Rest Encryption
2. Lack of Locks in Racks
3. Plaintext Protocols for Testing Network
4. Default Credentials

**Table of Findings**

**(U//FOUO) LACK OF DATA AT REST ENCRYPTION**

- (U//FOUO) Posture: Nearsider
- (U//FOUO) Affected System(s): System 0 / 192.168.1.10:445, 34 / 192.168.1.20:80,443,8443
- (U//FOUO) Issue(s): Several unencrypted HDD found...
- (U//FOUO) Mitigation: Encrypt HDD

**Finding's Info  
(Hot, Issues,  
Posture,  
Mitigation)**

**(U//FOUO) LACK OF DATA AT REST ENCRYPTION**

Finding #0  
Screenshot #0

**Screenshots**

**(U) OVERALL OBSERVATIONS**

- (U//FOUO) System Strengths
  - (U//FOUO)
  - (U//FOUO)
- (U//FOUO) System Weaknesses
  - (U//FOUO)
  - (U//FOUO)
- (U//FOUO) Overall Mitigations
  - (U//FOUO)
  - (U//FOUO)

**Overall Observations**

**(U) POST ASSESSMENT REPORTING**

- (U//FOUO) Emerging Results Brief (ERB)
  - (U) List of findings with minimal analysis
  - (U) Overall assessment objective completion status
- (U//FOUO) Risk Matrix
  - (U) List of findings with technical risk levels
- (U//FOUO) Technical Report
  - (U) Option A → Technical Memorandum ~30 working days
  - (U) Option B → Published Report ~90 working days

**Post Assessment  
Reporting**

**(U) CONTACT INFORMATION**

Salvador Melendez, CISSP, CJEH, Sec+  
UNCLASSIFIED: xxxxxxxx.civ@mail.mil  
SIPR: xxxxxxxx.civ@mail.sml.mil  
O: (575) xxx-xxxx  
M: (975) xxx-xxxx

**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](mailto:salvador.melendez3.civ@army.mil)