TASKS COMPLETED BY BY RED TEAM TNB INTERNS

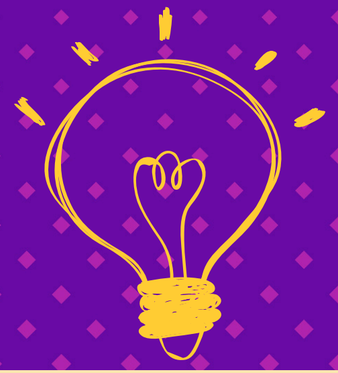
Date : 15 January 2025

By Muhammad Qayyim bin Khamarudin
Matric No: A21EC0090
Course: SECRH/4

TABLE OF CONTENT

VULNERABILITY ASSESSMENT PROJECT

RED TEAM RECONNAISSANCE PROJECT



VULNERABILITY ASSESSMENT PROJECT

INTRODUCTION

PURPOSE

To develop a method for the Vulnerability Assessment Team's results reporting to be done from Excel to Outlook in a steadfast manner. Such automation is for distribution to the necessary recipients can be done, streamlining the task, and reducing time consumption.

ABOUT

The Outlook mail generated from the results via Excel is designed in a pre-determined format template. The necessary requirements were also applied in the automation process, such as activating the reminder setting for the recipients and flagging the mails as "High Importance".

PROBLEM STATEMENT

1. Time-Consuming Manual Email Preparation Process

2. Inconsistent Formatting and Human Errors

REQUIREMENT GATHERING

Method of User Requirements Gathering :

- Stakeholder Meetings & Discussions

List of User Requirements :

- Macro Button
- CVE Code Selection and Data Extraction via Macro
- Dynamic Column Identification
- Inclusion of Asset Affected Table into the Email Template
- Body Message with Formatting and Color
- Set Outlook Email as "High Importance"
- Outlook Email Generation

TOOL DEVELOPED

WHAT?

Excel to Outlook Report Automation Tool

WHERE?

From : Excel
To : Outlook

WHY?

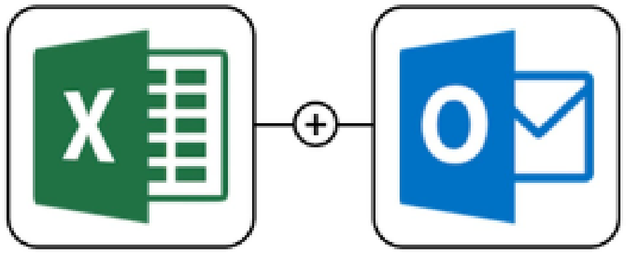
- To allow the VA Team to create an Outlook report based on the pre-determined format containing the selected data via automation.
- To prevent human error during reporting.
- Less time-consuming.
- Minimize effort.

WHEN?

Vulnerabilities Reporting Phase

HOW?

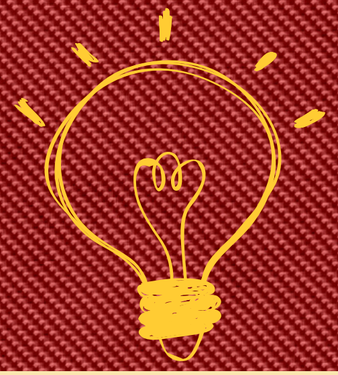
Enable automation just with the click of a few buttons



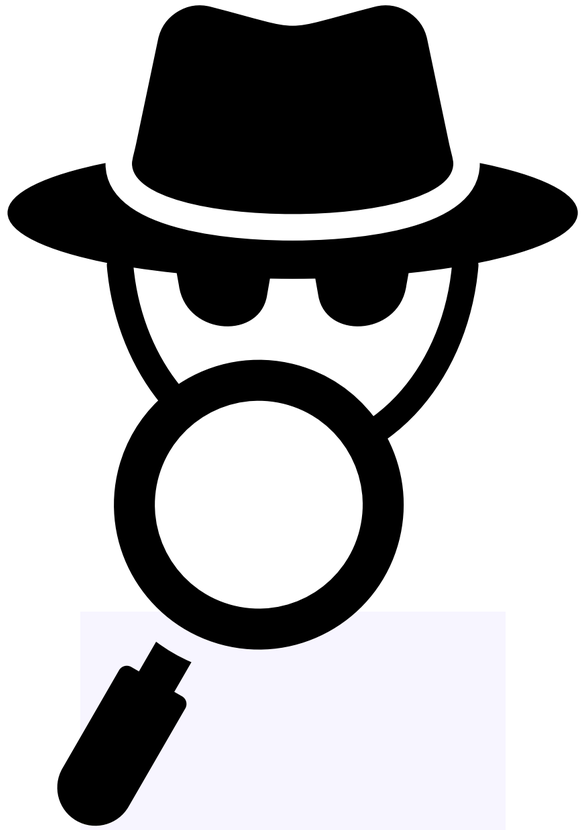
TOOL DEMONSTRATION

CONCLUSION

In conclusion, the Vulnerability Assessment Team's Excel to Outlook Automation Project has been successfully completed, streamlining a previously redundant reporting task. The user requirements were thoroughly met, resulting in a solution that not only saves time but also reduces manual effort and minimizes the risk of human error. By automating the process, the team can now focus on higher-value tasks, leading to increased efficiency and accuracy in vulnerability reporting. This project marks a significant improvement in workflow management and serves as a model for future automation initiatives within the organization.

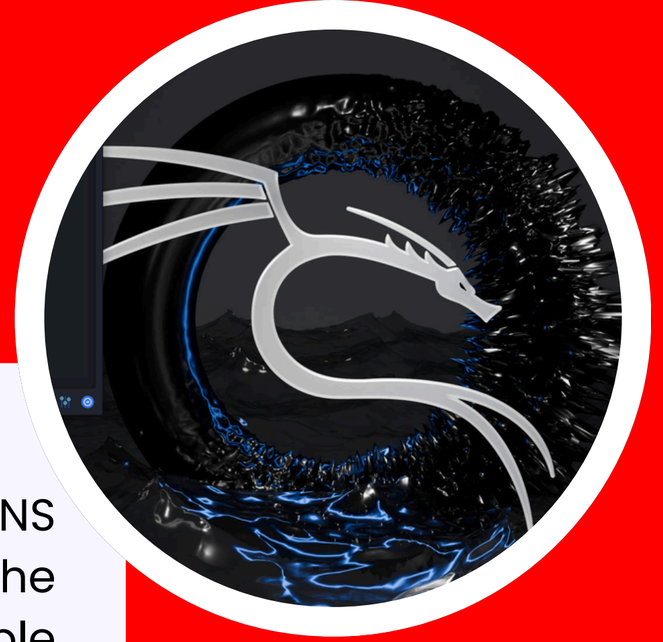


RED TEAM PROJECT



RECONNAISSANCE TOOLS

INTRODUCTION



ABOUT

The tool integrates multiple reconnaissance utilities (WHOIS, ARIN, DNS Resolver, Subdomain Enumeration, theHarvester, crt.sh, and VirusTotal). The combined reconnaissance tool automates data collection from multiple sources.

PURPOSE

To deliver comprehensive reconnaissance results, including emails, DNS records, HTTP/HTTPS URLs, IP addresses, hosts, ASNs, and insights on malicious or suspicious activities, ensuring efficient and accurate data collection.

PROBLEM STATEMENT

MANUAL INFORMATION GATHERING

TIME CONSUMING PROCESS

PRONE TO HUMAN ERROR

REQUIREMENTS GATHERING

Method of User Requirement Gathering

- Stakeholder meetings and discussions

List of User Requirements

- Input Field for Domain/IP Address
- Run Reconnaissance button function
- Export Results to CSV button function

TOOL DEVELOPED

WHAT?

Reconnaissance Automation Tool

WHERE?

From : Kali
To : Excel

WHY?

- The tool helps the Red Team easily gather detailed information like emails, DNS records, IPs, hosts, and malicious activity, saving time and improving accuracy for effective penetration.
- Prevent human error during reconnaissance.
- Less time-consuming and effort

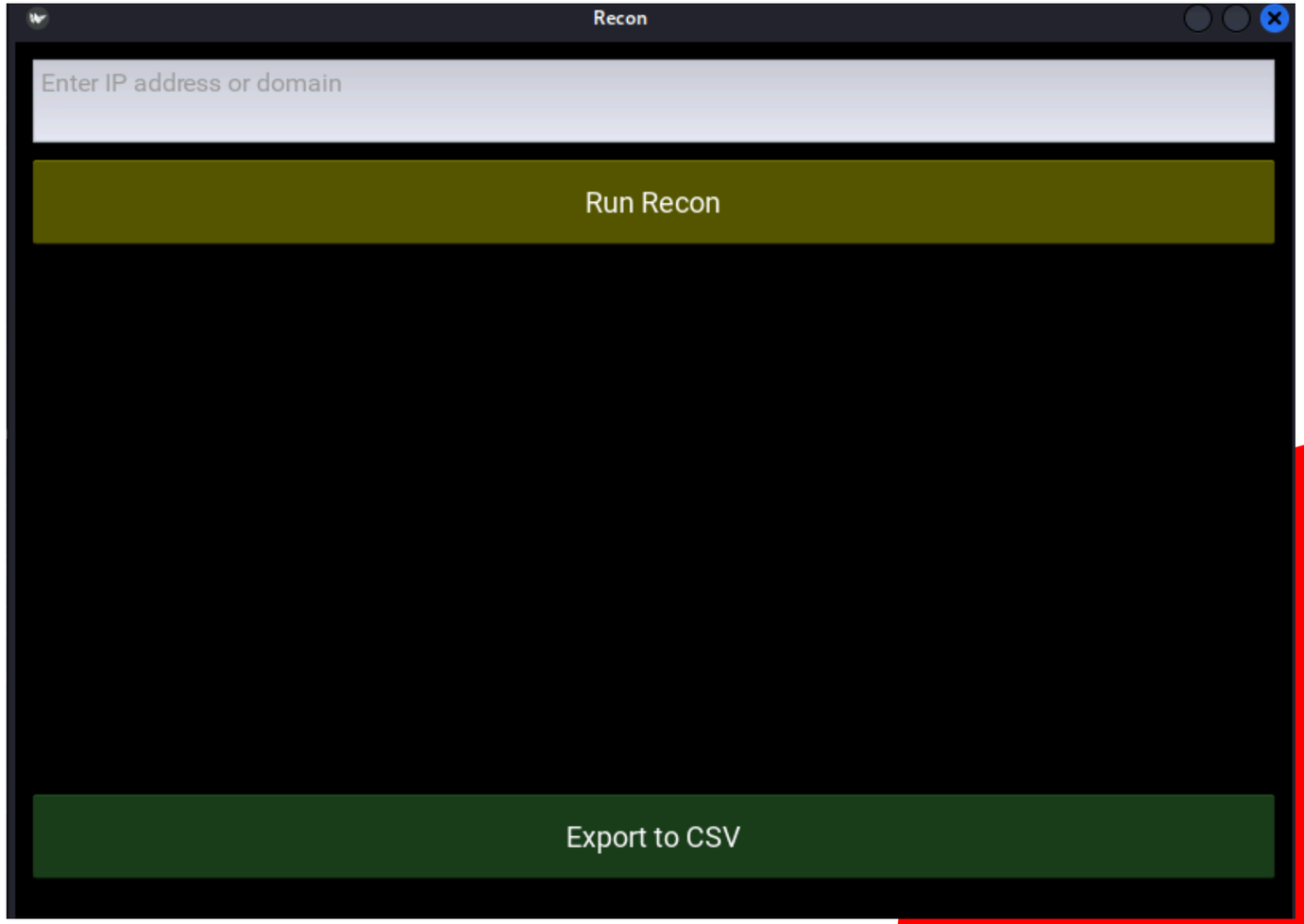
WHEN?

The reconnaissance phase of Red Teaming.

HOW?

Enable automation of information gathering with a click of a button.

TOOL DEMOSTRATION



CONCLUSION

In conclusion, the Reconnaissance Automation Tool has been successfully developed and implemented, addressing the challenges of manual and fragmented data collection. The tool significantly enhances efficiency and accuracy. This solution not only minimizes manual effort but also reduces the likelihood of errors, ensuring reliable results.

THANK YOU