Quick Reconnaissance Gathering Tool

Rakesh Kumar R[1], Priya N[2]

Jain (Deemed-to-be-University)
Department of MCA School of Computer Science & IT, Jain Knowledge Campus, Jayanagar 9th Block, Bangalore

---

ABSTRACT: Information gathering plays a major role in any sort of pen testing or information analysis process. This process consume a lot of time and needs enormous amount of effort from the pen tester end and utilizes various tools to gather certain set of information. This Project presents an approach to develop a quick information gathering tool which could be used in any circumstance reliably and efficiently where the time consuming process is less. This could also perform as a standalone software or can be used in modules with third-party by binding it together with the software and utilising its features. This could also eradicate the use of various pre software's which required to exploit a system or to find its vulnerabilities

INTRODUCTION

Information gathering is always a primary task for an attacker, ethical hacker or an investigation officer. There are various ways to gather information from a computer but none of them are straightforward they either have a roundabout method or intricate attack details just to gather some basic information about an information system. This closed source could help various officers to gather some specific information about a machine in a network in few seconds the recon tools which are available right now are so vastly spread in categories that we have to drop or use specific tools for specific purposes which ranges from a simple network monitoring to application monitoring and there is no all-in-one tool which could pull out or fetch information about a computer.

This could be sometime time consuming for an officer who is currently in a field or a network with an attacker with a limited amount of time. All these intricate details matter's either in a crime scene or at a place where the time is in limited amount

These things has to be resolved right we do not have to wait for the end to come with a solution or a program which uses such a huge amount of resources which could only provide us with just a small amount of data about the machine. So this tool could avoid time and also help us to save consume time in many precious cases where time matters a lot these new-gen info gathering tools has only specific system to carry out an information they all run in a very specific way to get embossed into some kind of file, but getting machine data without an administrator permission is really easy with this tool the simple bypass does that and gather those information in split seconds these could come handy in an emergency situation where we a are unable to know the password of the administrator but we still can gather those information with peculiar confidence with this tool.

The machines are always full of data or information which could be used by an investigating officer but retrieving it and compiling it into a human readable format within few seconds is always the crucial part in a tool it could take some minutes to hours or it could even fail due to various circumstances. This could be really a huge lead to the officer because the more the information he has the more it is easy to him to solve a crime or stop an attack.

AIM OF THE PROJECT

The core objective is to create an information gathering tool which could fetch out all the crucial information out of an information system within few seconds without any other alternatives and work efficiently.

SCOPE

- Current information gathering tool doesn't jump down deep into windows to gather info about a pc
- This tool doesn't need any other third part side-loading
- User friendly

PROBLEM STATEMENT

- To design an Information Gathering tool which is fast and reliable and works even from a pen drive and saves a file to it
- Fundamentally it is a Windows Information and Log Saver
- The tool runs deep down to admin level to gather information with admin permission

PROPOSED SYSTEM

The proposed system is an information gathering tool, which uses built-in windows features to gather various details about the computer. The tool is segregated in various parts as it could be used as a

stand-alone tool and it also could be used as a side loaded payload which could run in any of the content delivering payload mechanism to gather information from a computer. Thus it could work as a tool for a security officer or a pen tester. The tool does a deep down scan throughout the computer system and provides us a report in a designated order. This tools is designed to minimize all of these possible factors and helps to gather information from a machine by efficiently consuming the users time and providing with more beneficial data which could be further used or enhanced to plan attacks or to plan their next step over the machine

METHODOLOGY

The main contribution of the proposed system is three components:

Batch script – Performs the intended system information discover method

System Information – Built in windows tool extracts all the required details

Extractor – Saves all the data to an output file and proceeds to verify the integrity of the file

Content Saving management –Drops down the file to the place it has been prompted

Quick Reconnaissance helps us to gather Information in a minimal time from a windows computer system using basic scripting mechanism and also helps us to track the hidden basic system info which are sometimes overlooked up many security officers in the process of scanning. Quick Recon doesn't give a chance to them it entirely compiles the whole system information into a solid notepad file with two more basic files and saves them in a specific place which we have requested.

It uses built in windows system information gathering tool to request a system wide detail gathering session and extracts them to a notepad file and the sys info plays a major role of contributing to this operation. The built in tool solves us a lot of times instead of using python to import sys tools to even extract a basic set of information. These tool is automated for our specific needs. It also can be modified according to our need

This tool extracts the info and our extractor does that in a safe and secured manner with accurate precision these tools could be combined and made sure to create a successful task even without any prior experience

Content saving management helps to create many files to perfectly store our report file. It creates an msreport sys info file which you could also use to open in any windows computer using sys info to look up into the system to extract the details.

LITERATURE REVIEW

1. Abhilash S S, Lisho Thomas, Winquisitor: Windows Information Gathering Tool by Micheal Cardosa

- The same root concepts where the information about a windows system is gathered in a timely manner
- Helps administrators to monitor system and prevent any attacks or to respond immediately to threats which occur in the system
- It also works as a remote system access tool but needs permission to perform operations successfully
- **Pros** – Acts as a Good Info-Recon Tool
- **Cons** – Needs admin permission or system credentials to gather and perform various operation**s**

Dmitry

DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU) Linux Command Line program coded purely in C with the ability to gather **as** much information as possible about a host. DMitry has a base functionality with the ability to add new functions.

- The basic functionality of DMitry allows for information to be gathered about a target:
- Providing a deep information from a network stand point of view rather than host standpoint of view
- Uses systems network layer (TCP/UDP) level to gather and transfer detailed information

Windows Management

Instrumentation

Windows Management Instrumentation consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

DISCUSSION

Quick Recon is an effective way for people to gather system information in the computers in a fast and secure manner with low error rather. A technical approach is usually utilized to increase the performance of the tool.

According to literature review. The existing system has a drawback for using admin permission for even gathering basic system information which may result the complication of the process without right user account or with admin privileges too. This technique eliminates the use of admin permissions without and captures the system information without even having a huge benefits from the tool. The reaping script performs the information gathering method for various details from the system. This system has a broad rand of use cases.

ahmad, hasan kahtan, fadhl hujainah, and hamid a. Jalab

CONCLUSION

In this project, our core intention was to gather system's information in an efficient manner which could fetch out all the basic and advanced details, without any third party software's installed inside an another computer and this tool could also play as a standalone tool which could be performed from a thumb drive or also dropped inside a network or also work as a third party module which could be performed with already available famous tools like Metasploit, etc.

REFERENCES

[1] Global Information Assurance Certification Paper Copyright SANS Institute Author Retains Full Rights, Author: Mike Cardosa, mcardosa@gmail.com Advisor: Rick Wanner

[2] Sudomy: Information Gathering Tools for Subdomain Enumeration and Analysis, the 2nd International Conference on Engineering and Applied Sciences 2019 (2nd InCEAS 2019)

[3] A fresh new look into Information Gathering, Christian Martorella IV OWASP MEETING SPAIN

[4] Effective information gathering on the web BY Anwar Alhenshiri, Carolyn Watters, Micheal Shepherd, February 2015

[5] Exploring Information Gathering Process in Networked Environments Petek AKAR, Arif altun, vildan cev_k1

[6] Systematic literature review on penetration testing for mobile cloud computing applications ahmad salah al-