RECO

RECONNAISSANCE TOOL

NOOF ALGHUFAILY,NOOF ALMAHASHEER ,FATEMA ALMASSARY
RENAD ALGHAMDI ,RENAD ALQAHTANI
MR.HUSSAIN ALATTAS

INTRODUCTION

RECONNAISSANCE IS THE PRACTICE OF MONITORING THE TARGET'S SYSTEM AND GATHER INFORMATION ABOUT IT.
RECONNAISSANCE APPROACHS BASED ON HOW INFORMATIONS GATHERED:
-LOGICAL APPROACH ----> BY PROBING THE NETWORK.
PHYSICAL APPROACH ----> BY SOCIAL ENGINEERING.

RECO IS A TOOL THAT PERFORMS A LOGICAL RECONNAISSANCE. IN RECO TOOL, THERE ARE TWO MAIN CHOICES FOR THE USER, EITHER THE USER ENTERS AN IP ADDRESS TO RUN DIFFERENT TYPES OF SCANS ON IT, SUCH AS TCP SCAN, UDP SCAN, COMPREHENSIVE AND REGULAR SCAN. OR ENTER A DOMAIN NAME TO RUN A DNS LOOKUP, WHICH WILL PREVIEW INFORMATION DETAILS ABOUT THAT DOMAIN NAME.

MAJOR THREATS

THE GATHERED INFORMATION CAN BE USED TO FURTHER STRENGTHEN ATTACKS SUCH AS:

DOS (DENIAL OF SERVICE) WHICH IS PERFORMED BY SENDING A FLOOD OF PACKETS TO A PARTICULAR SYSTEM, THIS CAUSES A SYSTEM TO SUDDENLY CRASH.

SENSITIVE INFORMATION ABOUT THE TARGETED SYSTEM OR ORGANIZATION MIGHT BE EXPOSED.

COUNTERMESURES

IT IS HARD TO COMPLETELY PREVENT SUCH ATTACKS LIKE RECONNAISSANCE, BUT THERE ARE SOME METHODS TO FOLLOW THAT MAKES IT HARDER TO PERFORM THESE ATTACKS , SUCH AS:

- **SNIFFING AND SCANNING PREVENTION:** IT DISCOVERS IF THERE ARE ANY WEIRD NETWORK INTERFACE CARD IS SET TO PROMISCUOUS MODE, THAT IS, ALL THE RECEIVED FRAMES ARE PASSED TO THE HIGHER LAYERS OF THE PROTOCOL STACK DESPITE THE HOST IS NOT THE INTENDED DESTINATION.

- **CYBER DECEPTION:** IT PROVIDES THE ATTACKER WITH A MISLEADING INFORMATION TO DECEIVE THEM, OR TO MANIPULATE THE NETWORK TRAFFIC TO DELIVER THE ATTACKER TO A VIRTUAL AND USELESS NETWORK TOPOLOGY.

- **FIREWALL** SHOULD BE CONFIGURED TO ALLOW ONLY NECESSARY TRAFFIC AND ALSO CONFIGURED TO LOG MULTIPLE CONNECTIONS FROM THE SAME IP ADDRESS

Refrences:
[1] S. Micallef, "SpiderFoot automates OSINT collection so that you can focus on analysis. | PythonRepo", Pythonrepo.com, 2021. [Online].
[2] thewhiteh4t, "Thewhiteh4t/finalrecon: The last web recon tool you'll need," GitHub. [Online]. Available: https://github.com/thewhiteh4t/FinalRecon.
[3] Smicallef, "Smicallef/Spiderfoot: Spiderfoot automates OSINT for threat intelligence and mapping your attack surface.," GitHub. [Online]. Available: https://github.com/smicallef/spiderfoot.

SPIDERFOOT TOOL

- AN OPEN SOURCE INTELLIGENCE AUTOMATION TOOL THAT UTILIZES A RANGE OF METHODS FOR DATA ANALYSIS.
- IP ADDRESSES, DOMAIN NAMES, E-MAIL ADDRESSES, AND MORE ARE SOME PIECES OF INFORMATION THAT CAN BE REVEALED. [1]

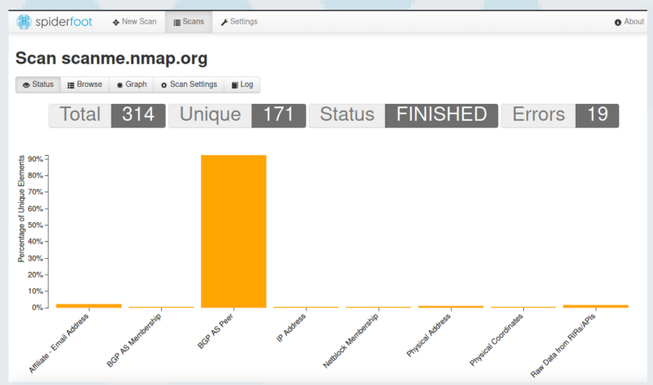
MAIN COMMANDS:

Web UI Model-

- *~/spiderfoot$ python3 sf.py -l 127.0.0.1:5001*

Once executed, a web-server will be started, which will listen on 127.0.0.1:5001. You can then use the web-browser of your choice by browsing to https://127.0.0.1:5001.

AFTER CONDUCTING THE SCAN ON A TARGET, A GRAPH INCLUDING INFORMATION ON THE CURRENT STATUS OF EACH MODULE. WILL APPEAR .



FINALRECON TOOL

- INCREDIBLY SIMPLE, COOL TOOL TO INSTALL.
- AN AUTOMATIC WEB RECONNAISSANCE TOOL THAT IS WRITTEN IN PYTHON.
- PROVIDES AN OVERVIEW OF THE TARGET IN A SMALL AMOUNT OF TIME WHILE MAINTAINING THE ACCURACY OF THE RESULTS.

MAIN COMMANDS:

- *python3 finalrecon.py --headers <target URL>*

get valuable header records, such as server information, scripting language, and content-encoding technique.

- *python3 finalrecon.py --ps <target URL>*

The port scanning module scans the top 1000 ports and presents the results in this format, port num: service name.

COMPARISON

FINALRECON [2]	SPIDERFOOT [3]
- Header Information	- Suports Over 200 modules, so it can perform finalrecon's features and more
- whios	- Visualisations
- Crawler	- Multi-target scanning.
- SSL Certificate Information	- Bitcoin address extraction
- DNS and Subdomain Enumeration	- Web based UI or CLI
- CLI	- Free with limitation / subscriptions
- Port Scanning	- CSV/JSON/GEXF export
- Free	
- txt/xml/csv export	

CONCLUSION

RECONNAISSANCE IS ONE OF THE MOST IMPORTANT BUT ALSO MOST TIME CONSUMING PART OF PLANNING AN ATTACK OR PENETRATION TESTING. THANKS TO THE VARIOUS RECON TOOLS, TIME FOR SEARCHING IN WEBSITE OR SERVER VULNERABILITIES HAS REDUCED SIGNIFICANTLY.