IJCRT.ORG ISSN : 2320-2882
INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Information Gathering and Vulnerability scan Tool

Meena Yogesh, Urmila Ghallay

[Students of School Of Computer Science and Engineering]

Lovely Professional University, Phagwara

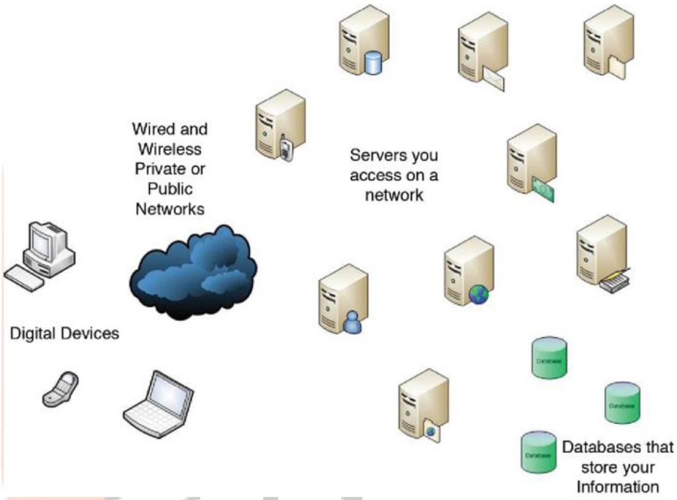
Abstract—

When we conduct digital surveillance and reconnaissance,
the focus is to gather as much information as possible. Doing so is no simple job. However, because we are in this digital world, the job is made much easier. For an instance, a phone can be bugged with a device to sniff any conversation made by the phone. Just like that, we have developed a tool that lets the end user to gather any kind of information, those stored on social networking and sites within minutes by simply sitting at one end of your computer terminal and connecting yourself to the internet.
Moreover, it also lets you automate scan and automate attacks on the target. This tool is also a solution to many existing problems such as finding your device or site's security flaws, insecure devices, passwords, and reports.

Keywords— **Reconnaissance, information Gathering, Automation attack, End User, penetration testing.**

I. INTRODUCTION

Your actions within the digital domain can be stored. From posting a picture on a social media to accessing your mobile phone, using geo locations.


Wired and Wireless Private or Public Networks
Servers you access on a network
Digital Devices
Databases that store your Information

In the above diagram, a view of all the points that can store data is shown. Every one of these points can also be used for information gathering. Here we can see how digital devices are connected to a network to use resources, for instance, uploading a file, accessing a website, sending an email and much more. Thus, every transmission that takes place leaves behind evidence and the activity can be captured.

All in all, to protect yourself from being spied on, you need to limit your exposure. Our daily habits can easily track us down.

If someone wants to spy on a company. He/she can easily do it by gathering publicly available information using tools such as Whois Domain.

There is no shortage of information availability on the internet including social media, job posting boards and metadata attached to files, documents and pictures. The only purpose of information gathering is in order to understand the working of a target system and discover its security lacks.

To start off the process, we first collect the information about the target. It is done in two ways:

1. Passive Information gathering- in this approach only the publicly available information is gathered. The interaction between target is nil. Example: whois domain, social media networks.

2. Active Information gathering- it requires more preparation since active interaction with target is required in the approach. Due to this it can trigger alerts to the target. Example: open ports, services, version of target operating system and applications.

This information collected can be later used to study the target. It is the initial steps towards any planned vulnerability exploit. Given the digital advancement of today, to perform any attack can be quite easy even for newbies, using automated tools. However, the existence of automated tools have not been popular enough. We have tried to come up with our very own idea of automation tool, which is much handy and user-friendly.

II. Objective

1. To create a platform which is simple and user friendly.
2. To create a platform which can be afforded by all small level business entities.
3. To create awareness about the importance of cyber security.
4. To make a platform which is cost efficient and can be useful for any small business or company who wants to secure their system.
5. Scans system for its vulnerability and suggest exploits and bug fixes for the vulnerability.
6. Generate payload according to system architecture.
7. By using open-source intelligence, we can collect required data from publicly available sources.

III. Existing System

Maintaining an organization’s security comes very expensive and requires a lot of time and effort. It requires the company to hire a third-party agent to conduct the security analysis.

The penetration testing identifies a target system and define goals. The team then performs an assessment of the organization determining if the system is vulnerable enough to be attacked by some third person or not. The test also identifies any potential impact of these vulnerabilities to the company and recommends remediation accordingly and fixes the vulnerabilities.

Penetration testing is broadly defined as a method of testing an organization’s data defense using a controlled ethical hacking environment. The objective of penetration testing is to find any weak spot in the target system’s defenses which the attackers might take advantage of.

The scenario can be related as a bank hiring someone to disguise as a burglar and try to break into their building to gain access to the vault. If the burglar succeeds to get into the bank, the bank can note down those weak spots where they need to tighten their security measures.

IV. Problems in the Existing System

The process to conduct cyber security analysis is time taking. During the process, the office work gets disturbed depending on the in-depth security analysis being performed. Not only this, but the cost of the process overall is also very expensive.

The small companies cannot afford the expenses of the entire process. Thus, the security of their organization is at stake.

With the rise of threats nowadays, there are many ‘would be cyber’ companies jumping on the cyber security bandwagon. They tend to offer a variety of solutions, often ill equipped and lacking the proper experience.

V. Proposed System.

Information gathering and vulnerability scan tool is a custom bash scripts used to automate various penetration testing task including recon, scanning, foot printing (using public data) and creating malicious payloads and listeners with Metasploit. It is used with kali Linux and the penetration testers framework. This tool is built to make penetration testing and information gathering easier as user have to only input required details and bash script will perform process. In the end it will generate report and present it to end user.

VI. Methodology

The project has been divided into different modules and respective sub modules.

Reconnaissance

First module and very initial step of the tool. This module has been further divided into 3 sub-categories:

1. Domain
2. Person
3. Geoscrapper

I. Domain

It gives user two options to look for.

a. Passive:

Passive information gathering does not involve any direct contact between the target and attacker. It does not require any interaction with the target system. You can collect as much information as possible from the public data sources like social media, hibp, intelligence X and much more.

In this module, we have made use few of the tools to grab public information. It includes, Amass, theHarvester, DNSrecon, goofile, Metasploit, whois, DNSdumbster, recon-ng.

b. Active:

Whereas in case of active information gathering, it requires active contact between attacker and the target. For instance, Nmap allows running scans on the target system. It returns with open ports and applications running on the system. Thus, here the attacker is interacting with the system by sending special packets.

Tools used are traceroute, Zone Transfer, whatweb, recon-ng.

The given domain is ran by several tools mentioned above and the final output is generated. The final output is of various types, some files containing information about the sub-domains, MX records, pdfs, whois data, etc.

II. Person:

This module covers information gathering about the person. An input from a user is asked, that is, any username he/she wants to grab data about. The system takes in the username and searches over several tools including all social media platforms where the given username has been used. The found profiles are then listed and an outfile file is generated.

III. Geoscrapper:

As the name suggests, this module only covers location-based data. We have utilised API keys provided by users to access data from web servers and data is sorted accordingly given the location input by the user.

Recon-ng together with pushpin module allows to pull data from various social media sites such as Flickr, YouTube, Twitter and much more. The collected data is correlated with geolocation coordinates, pulling up a map pinpointing the land around the target.

What happens is when we take pictures or tweet, our smartphone automatically embeds coordinates into the picture or tweet. Thus, allowing geolocation tools to access them.

Location services has pros and cons. Finding a restaurant nearby with good reviews or proving where you can be helpful. On the other hand, it can prove to be weakness of a company when this information such as pictures and videos of the company gets into the hands of a bad guys.

Automation Attack

In everyday life, humans one way or another interact with IoT devices. Every device runs on an operating system and a program. Time to time it needs an update so in order to test vulnerability and identify program technologies used in it. If the program have outdated configuration or program or operating system an attacker will be able to exploit the device.

Modules included in this section are:

This second module is further divided into:

IV. SSL vulnerability

This part deals with vulnerability assessment of websites. It takes input from the user for which he or she wants to test the vulnerability of the website. The tool checks for different kinds of vulnerability like heartbleed and all.

V. Generating malicious payload and listners

For a pen tester to generate payload each time he/she decides to exploit a system, can be hectic. Every system will have different vulnerability and needs to generate payloads accordingly. So this tool overcomes the shortcoming, making an end user to only provide IP address.

VI. Live system test

As the name suggest, it detects for live systems which are active in a particular network of an organization and list them in the output.

VII. Exploit suggester (smart Nmap)

It is just a simple script that keeps track of vulnerabilities. At the same time, it also suggest possible exploits of the system.

VII. Project Outcome

As not all small businesses can hire an ethical hacker or penetration tester this tool will help them to check their own system security status. This tool will be helpful for professional as well as those who are new to cybersecurity. Plus, it is going to be a time saver tool.

Our motive behind this project is to make things easy for end user. For instance, if a user wants to scan his system or scan a server or website before using it, our tool will turn out to be very useful for them in finding out whether the system is secure or not. In case of a website, it will tell them whether the website is fully secured or not.

VIII. S/w and H/w Requirements

1. **Environment:**

- **Servers:**
- **Operating System :** Any linux based os
- **Clients** **:** Firefox
- **Tools** **:** Visual Studio, Brackets
- **User Interface:** HTML 5, CSS, JavaScript, terminal.
- **Code Behind** **:** Python, Bash

2. **Requirements**

- **Hardware**
  - ○ **Processer:** - Intel i3 or higher
  - ○ **Hard Disk Space: -** 20 GB and more
  - ○ **Ram Memory: -** 4 GB and Higher

IX. Conclusion

To wrap it up, firstly, information gathering can be of great deal to us during automation attack. It allows us to collect information on people, systems and networks which are indeed our very target which makes it easier to attack them. Secondly, there might be many other potential uses of the information we have fetched but the two most important uses are social engineering and footprinting of the target for attack. Carefully examining the gathered information, we can identify the vulnerability and exploit them with the required tool.

The above summarised detail is the new innovative tool of the future hopefully. If the idea is implemented in a broader perspective, it can do more than it is being explained. With the world turning digital today, it is a small contribution towards the digital world. Every work we do nowadays is focused on reducing the workload on humans, making it easier and simpler.

Abbreviations
DDoS: Distributed Denial of service
Nmap: Network mapper
PVS: Passive Vulnerability Scanner
SSL: Secure Sockets Layer
MX: Mail Exchanger
DNS: Domain Name System

X. Reference

[1] CPNI and Homeland Security. (2010) "Cyber Security
Assessments of Industrial Control Systems", Control Systems
Security Program &amp; National Cyber Security Devision,
https://scadahacker.com/library/Documents/Assessment Guidance/
DHS.

[2] M. Franz, “Vulnerability Testing of Industrial Network Devices,” in *ISA industrial network security conference, Critical Infrastructure Assurance Group (CIAG)*, Cisco Systems Inc., 2003.

[3] M. Evans, L. A. Maglaras, Y. He, and H. Janicke, “Human behaviour as an aspect of cybersecurity assurance,” *Security and Communication Networks*, vol. 9, no. 17, pp. 4667–4679, 2016.

[4] N.Ayres and L. A.Maglaras, “Cyberterrorism targeting the general public through social media,” *Security and Communication Networks*, vol. 9, no. 15, pp. 2864–2875, 2016.

[5] D. Duggan, M. Berg, J. Dillinger, and J. Stamp, *Penetration Testing of Industrial Control Systems*, Sandia National Laboratories, 2005.

[6] P. Kerr, J. Rollings, and C. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, Congressional Research Service, 7-5700, 2010, http://www.crs.gov.

[7] S. Samtani, S. Yu, H. Zhu, M. Patton, andH. Chen, “Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques,” in *Proceedings of the 14th IEEE International Conference on Intelligence and Security Informatics, ISI 2015*, pp. 25–30, USA, September 2016.

[8] R. C. Bodenheim, *Impact of the Shodan Computer Search Engine on Internet-Facing Industrial Control System Devices*, Air Force Institute of Technology, 2014.

[9] N. R. Rodofile, K. Radke, and E. Foo, “DNP3 network scanning and reconnaissance for critical infrastructure,” in *Proceedings*

Security and Communication Networks 21

of the Australasian Computer Science Week Multiconference, ACSW 2016, February 2016.

[10] G. Bartlett, J. Heidemann, and C. Papadopoulos, “Understanding passive and active service discovery,” in *Proceedings of the IMC’07: 2007 7th ACM SIGCOMM Internet Measurement Conference*, pp. 57–70, October 2007.

modeling for performance and vulnerability assessment of integrated cyber-physical systems,” *International Transactions on Electrical Energy Systems*, vol. 25, no. 3, pp. 498–519, 2015.

November 2010.

[11] J. Gonzalez and M. Papa, “Passive scanning in modbus networks,” *International Federation for Information Processing*, vol. 253, pp. 175–187, 2007.

[12] N. R. Rodofile, K. Radke, and E. Foo, “DNP3 network scanning and reconnaissance for critical infrastructure,” in *Proceedings of the theAustralasian Computer ScienceWeekMulticonference*, pp. 1–10, Canberra, Australia, Feburary 2016.

[13] R. Deraison and R. Gula, *Blended Security Assessment: Combining Active, Passive and Host Assessment Techniqiues*, Revison 10, Tenable Network Security Inc, 2011.

[14] D. Peterson, “Using the Nessus Vulnerability Scanner on Control Systems,” *Digital Bond Inc*, 2006.

Conference, pp. 542–553,Denver, Colorado, USA,October 2015.

[15] F. Li, Z. Durumeric et al., “Youve Got Vulnerability: Exploring Effective Vulnerability Notifications,” in *25th USENIX Security*