ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/357835928

Technical Methods of Information Gathering

Article · January 2022

DOI: 10.37591/JoWET

CITATIONS
0

READS
3,419

2 authors:

Dhaval M Chudasama
Indrashil University
41 PUBLICATIONS **196** CITATIONS
SEE PROFILE

Rakesh Bhavsar
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Project Information Systems Audits for eCommerce View project

Project Grocery Deals View project

All content following this page was uploaded by Rakesh Bhavsar on 12 May 2022.

The user has requested enhancement of the downloaded file.

STM JOURNALS

Journal of
Web Engineering & Technology

ISSN: 2455-1880
Volume 8, Issue 3, 2021
DOI (Journal): 10.37591/JoWET

http://computers.stmjournals.com/index.php?journal=JoWET&page=index

Research JoWET

Technical Methods of Information Gathering

Dhaval Chudasama[1,*], Rakesh Bhavsar[2]

Abstract

Information gathering techniques are widely spread around the world. This technique is used by people to work accordingly. Something like this website & software development is used technique in the analysis of the project, also is it doing filed according information gathering ex. civil industries projects got this type of information collected. Here in the paper discussed by the cyber security field. In this field multiple techniques are available but I suggested the best technique for the network-based, DNS-based, Web-based etc. Also suggested various scanning methods like port, network, vulnerability, and provide various enumeration methods from your system safe to the attackers like this machine name, system name, Ip address, network resource, share and services. In this paper technique is more useful for industrialists and professional people. Information gathering technique derived steps are given to dictate the various attacks and organizations taking the safety steps. Hackers are done with Information gathering techniques targeted at people or systems. Steps of the Information gathering techniques are necessary for saving your devices, network, website, software to the hackers. Strong Information gathering techniques develop for your organization, no one can hack your networks or systems. You can apply auditing in your organization to save from hackers.

Keyword: Information gathering techniques, cyber security, information collection, information auditing, cyber reconnaissance.

INTRODUCTION

This technique is the collection of the information against the targeted person or organization. As a new ethical hacker performs various crucial steps, first you collect more content. Information gathering techniques are a part of security checking. Every hacker should master penetration testing [1]. All are aware of various tools, techniques and website, hackers gain help for gathering information such as a who is lookup tools. This step is needed for the Information gathering techniques like pet name, friend name, age, phone number, address, password or other attacks. Information gathering techniques are today's business and organizations. It is connected to their customers, users, employee, vendors and competitors. Information gathering techniques are relation sheets between information and organization for its improvement and also safety from the attacks [2].

Information gathering techniques in cyber reconnaissance are the basic step of the testing. In this section, Information gathering says about the target possibility. It is derived from the network topology and systems. This information is those staff members, customers, vendors, production, financials inventory, etc. This type of information is needed for hackers. This Information gathering technique is easy to organize attacks on the victim or organizations [3].

***Author for Correspondence**
Dhaval Chudasama
E-mail: dhavalchudasama16@gmail.com

[1,2]Ph.D. Scholar, Department of Computer Science and Engineering, Indrashil University, Rajpur, Kadi, Mehsana, Gujarat, India

Received Date: June 03, 2021
Accepted Date: November 28, 2021
Published Date: December 31, 2021

Citation: Rakesh Bhavsar, Dhaval Chudasama. Technical Methods of Information Gathering. Journal of Web Engineering & Technology. 2021; 8(3): 1–5p.

THERE ARE TWO TYPES OF RECONNAISSANCE.

Passive Cyber Reconnaissance

In this type of method Information gathering techniques direct interacting targets. Nothing to send an acknowledgment to the target and Information gathering on them. Using Information gathering

© STM Journals 2021. All Rights Reserved

public resources is called open-source intelligence osint we can gather information such as IP Address, domain name, email address, name, hostname, DNS records, running software, running website. Some passive tools for Information gathering techniques such as Google hacking, Net craft, Shodan [4].

Active Cyber Reconnaissance

It works directly within the system to gather computer-specific information about the target. This is works to gather devices that are connected to the same network. It is used to find out information like open/closed ports, OS of the machine, running services, host, or vulnerable applications on a host [5]. Active cyber reconnaissance is tools such as Nmap, Nessus, NIKITO.

Both the method difference is that Active cyber reconnaissance directly works with the system in order to system-level information while Passive cyber reconnaissance concern with tools on publicly available information for final results is that it is collected useful information through the given at least safe environment of the owner of the system activities.

LITERATURE REVIEW

Information is a weapon as we can believe most of the time you people believe the right time having the right information and especially knowing how to use it, that can be such as information is a weapon.

In cyber security, world information means any target person, company, domain name, or service is covered by parties. That is why the information gathering technique is one of the ultimate goal safety purposes and hackers for the malicious purpose [6]. If you gain as much information, as much as you reach the desired target. These are very time-consuming tasks during the Intel-recon process and that is why time management is so important. When you are getting clear information gathering, the simple way to define solve the problem. Various tools & techniques are available in the market here one review describes the how to get information [7].

1. **Social Engineering**: - in this method human mistakes give maximum data from the attackers like this in-person chat, phone conversations, and email spoofing.
2. **Search engine**: - Google hacking fetches information about anything about the company, person and service, etc.
3. **Social network**: - especially this platform through easily information gathering such as Face book, Twitter, LinkedIn, etc.
4. **Domain name**: This is registered by organizations such as government, public & private, and person. In this registration associated personal information, associated domains, technical & contact person information are found in the domain name.
5. **Internet servers:** - In this section, we discussed DNS servers are the big source of the information including related services such as HTTP, email.

There are lots of tools available for the information gathering technique, here we give information about the most popular tools of information gathering technique used by a cyber security researcher, academicians, industries person, etc.

1. **Nmap**: - overall network scanner data gathering tools. It is not used to scan ports and services fingerprints, but it works with DNS enumeration and network mapping tools.
2. **Unicornscan**: - It gives a clear picture of any remote network or host, it is able to work asynchronously stateless all TCP scanning with TCP flags, TCP banner grabbing, asynchronous UDP scanning, os fingerprinting, etc.
3. **Sublist3r**: - This is the best sub domain calculation tool around you and also helps create a virtual sub domain map of any website in no time if sub route integrity can perform a brute force sub domain discovery attack with wordlists. Using Google dark or others such as Baidu, Ask, Bing, and Yahoo.
4. **Dmitry**: - it is a good terminal-based tool while reconnaissance tasks. It allows you to get available

© STM Journals 2021. All Rights Reserved

data from any host, sub domain, email address, open ports, who is lookups, server data, and much more.

5. **OWASP Amass**: - it is helpful information gathering a create a full map of their digital asset for the perform DNS Enumeration, asset location, and overall attack surface discovery.
6. **Th3 inspector:** - it fetches all types of website-related information such as page data, phone number, IP address of HTTP, email server, who is lookup. Cloud proxy, age of domain name, scan remote active services, sub domain mapping, CMS detector, and much more.
7. **Devploit**: -this tool is given information about extract DNS, including DNS lookups, reverse IP info, port scanning, DNS zone transfer, HTTP-header, who is lookup, GEOIP lookup, subnet lookup, etc.
8. **Better crap:** -it is known as the knife of networking. It is powerful network recon, information gathering for Wi-Fi, Blue tooth low energy devices, and Ethernet network.
9. **Traceroute**: - it is a very popular network tool to track the path of network packets between one IP address to another, it is gain critical network information about IP addresses and networking request.
10. **WHOIS**: - it gives information of domain owner, booking data with expiry, register, technical, admin person contact data within a name, number, country, DNS server, etc.

RESULT & DISCUSSION

The results showed soul-searching, document analysis, and observation (passive) Shaft Ways/ tools aren't applicable in all four criteria of safety, mileage, learn ability, and Usability. These ways/ tools distance stakeholders from the Shaft process. Still, when safety is of concern to stakeholders, the critic should avoid the use of JAD sessions as studies have shown that people are more likely to be careful in such a group fashion so as not to upset superior associates, and hence is bad for managing stakeholders' cooperation and getting an overall understanding of stakeholders 'needs. In addition, utmost people generally feel unsafe when laboriously observed and accordingly bear in an extremely careful manner that could hinder the Shaft process [8]. At the other extreme, still, interview, questionnaire, stoner script, card sorting, laddering, and prototyping are least likely to produce safety enterprises for actors because these ways are generally conducted as a series of individual exercises. Also, card sorting, laddering, and stoner script ways give the stylish mileage for stakeholders. These ways have been developed with the end of knowledge elicitation and assaying the problem and what's the result sphere according to stakeholder's point of view. By keeping stakeholders' mileage high, it's largely likely that the stakeholders will cooperate and enhance the Shaft process. Also, interview (unshaped and semi-structured), prototyping, and JAD session give the stylish mileage as it gives an occasion to bandy in depth a stakeholder's studies and get his or her perspective on the business need and the feasibility of implicit results [9]. In discrepancy, structured interviews and questionnaires give the least mileage since the canvasser/ critic inventories the frame of reference for the polled/ repliers and is thus limited in the depth of knowledge they're suitable to evoke. Also, observation (active) isn't so helpful in understanding the conditions from the stakeholder's point of view.

Interview (unshaped and semi-structured), prototyping, and JAD session proved to be the most delightful, engaging, and stoner-friendly Shaft ways. Erecting an original prototype for the seeker conditions is useful for the client's satisfaction and 10 The IUP Journal of Information Technology, Vol. XIII, No. 4, 2017 for maintaining their feedback about as saying the current work. This process helps in numerous ways for streamlining, modifying, or indeed getting new conditions that the client needs [10]. Also, the informal approaches of unshaped and semi-structured interviews and the veritably interactive exercise of JAD insure a friendly, engaging Atmosphere for the stakeholders to be at ease during the Shaft process. Still, druggies are likely to feel uncomfortable when laboriously observed by judges, which accordingly will affect in a negative behavioral change and non-cooperativeness in the Shaft process. Further, the formal approach of the structured interviews makes the fashion boring for the polled. Also, the questionnaire lacks real- time stoner commerce. Card sorting, laddering, and stoner script ways fall in the middle. People find it easier and fun to relate to real- life exemplifications via stoner scripts, while the use of visual aids in card Sorting and laddering make the session engaging and satisfying for actors. Incipiently, for learn ability, the prototyping fashion is the most suitable fashion [11].

© STM Journals 2021. All Rights Reserved

A working model of the system is displayed, the druggies get a better understanding of the System being developed; therefore it ensures excellent stakeholders 'learnability. This is important for generating complete and precise conditions. Other helpful ways are interview (semi-structured and unshaped), stoner script, card sorting, laddering, and JAD. Interview (semi-structured and unshaped) and JAD allow for two- way communication and in- depth conversations that support the generation of new ideas and opinions. Other helpful ways for learn ability are stoner scripts, card sorting, and laddering. Stoner script makes it easier for stakeholders to learn, understand and condemn a stoner script of how they might interact with a software system. Also, card sorting and laddering encourage stakeholders to express knowledge in a way that supports literacy. Still, the use of structured interviews should be avoided since repliers aren't allowed to speak beyond the environment and compass of the design. Rather, in this fashion, the canvasser supplies the frame of reference for the polled. Incipiently, it's delicate for the party in the questionnaire to claw further into content or expand on new ideas. In the same way, they give no medium for the actors to request explanation or correct misconstructions. Web information gathering, although may indicate constantly searching the Web, is a complex task that goes beyond keyword hunt. The task has several subtasks which include conditioning that concern searching, re-searching, keeping, re-finding, managing, organizing, and comparing information. Web information gathering is exploratory and cognitively ferocious. Current Web tools present numerous difficulties to the stoner which requires that the stoner borrow varied strategies to manage with those. The exploration bandied in this paper introduced Web Gad, a prototype tool intended for perfecting how druggies gather information on the Web. Web Gad was intended to ameliorate how druggies to hunt, organize, manage, keeper-find, and compare information for information gathering tasks on the Web [12]. Web Gad is a tool with numerous capabilities that permit the stoner to perform multiple conditioning nearly contemporaneously without having to switch among multiple tools and operations while keeping the environment of the gathering process. Web Gad allows its druggies to keep not only individual runners but also information gathered for the task and stoner commentary and input along with a set of runners to represent the environment of a whole task. It also allows the stoner tore-find similar information by permitting hunt among task markers and taking the stoner back to the same gathering environment where the stoner left in a former Session. Also, the stoner can involve information from different saved tasks in the current task. The stoner can edit and format the information while viewing and searching further Web sources [9, 11].

Fresh Tools Information storehouse and browsing tools were linked as particularly important due to the electronic nature of the data sources. Because information dismissed as unconnected frequently proved to be more important latterly in their disquisition, the judges wanted tools that enabled environment-sensitive queries over the history of recaptured information. Similar IUI tools could allow judges to fluent lyre-discover former work. Another need linked by the judges is a tool for making together electronic information. The process of moving between electronic sources and a paper disquisition record proved onerous, indicating a strong need for intelligent operations that can help organize information within the environment of a disquisition. Information Sources all actors talked about the need for rich and dependable information sources. Framed astronomically, there were two orders of information sources (1) high- position background knowledge and (2) low- position event or factual information [10, 12]. Both types of coffers are essential tools for completing an analysis. In task one, corresponding to the early stages of an disquisition, the judges reckoned on high- position information to develop sphere-specific models. In task two, the druggies spent further time looking for low- position information as they gathered substantiation to support or refute the formerly- developed process model. Our compliances indicate that, despite the shift in focus between tasks, judges tightly couple their access to both data source types. As the judges discovered implicit substantiation, they would incontinently pierce advanced- position information sources to ameliorate their understanding of what they had plant. This hints that IUI tools for relating applicable data sources and integrating them into a invariant terrain would be extremely useful. Sphere Moxie another theme raised by the judges in our study is that of sphere moxie. Understanding the language associated with the Enron disquisition was a delicate task and all actors bandied the desire for direct collaboration with sphere experts. This

© STM Journals 2021. All Rights Reserved

highlights the cooperative nature of the information- gathering process and indicates a need for intelligent tools able of connecting judges to applicable experts. The creating of analysis templates, erected by sphere experts, also had broad interest from the judges in our study [4, 5]. These templates, designed for specific sphere problems, could be used to charge- swatch a disquisition in the early stages to give sphere beginners with formal models and ways developed by experts.

CONCLUSION

In this paper I have discussed various points, if you are focused on the Information gathering techniques in your organization from the breaching. You can apply this Information gathering techniques to your organization to collect system level information about your target operating system, target network systems, target active running machine and open / closed ports. If you do best practice on Information gathering techniques you save your network systems from the hackers.

REFERENCES

1. Baumann, S., Erber, I. & Gattringer, M. (2016) Selection of risk identification instruments. ACRN Oxford Journal of Finance and Risk Perspectives 5(2), pp. 27-41.
2. D M Chudasama, Darsh Patel, Abhishek Shah and Nihal Shaikh (2020), “Research on Cybercrime and its Policing ", American Journal of Computer Science and Engineering Survey, Vol.8, Issue.10, pp.14.
3. Maytorena, E., Winch, G. M. & Kiely, T. (2005). Construction risk identification. K. Kähkönen, & M. Sexton, Understanding the Construction Business and Companies in the New Millennium, pp. 304-315.
4. Soham Shah, M a Lokhandwala, D M Chudasama (2021) " *Decoding Farm Laws”, International Journal of Scientific Research and Engineering Development,* Vol.4, Issue.2, pp.590-595.
5. Chapman, R. J. (1998). The effectiveness of working group risk identification and assessment techniques. International Journal of Project Management, 16(6), pp. 333-343.
6. Ontario Human Rights Commission. 6. What is involved in collecting data – six steps to success [Online]. Available from http://www.ohrc.on.ca/en/count-me-collecting-human-rights-based-data/6-what-involved-collecting-data-%E2%80%93-six-steps-success
7. Security Made Simple. Active vs Passive Cyber Reconnaissance in Information Security [Online]. Available from https://www.securitymadesimple.org/cybersecurity-blog/active-vs-passive-cyber-reconnaissance-in-information-security
8. W3school. Ethical Hacking: Information Gathering Techniques [Online]. Available from https://www.w3schools.in/ethical-hacking/information-gathering-techniques/
9. Trocaire College. 10 STEPS OF THE RESEARCH PROCESS [Online]. Available from https://library.trocaire.edu/services/studentservices/researchassistance/10steps/
10. Security Trails. Information Gathering: Concept, Techniques and Tools explained [Online]. Available from https://securitytrails.com/blog/information-gathering
11. Java T Point. Methods of Information Gathering [Online]. Available from https://www.javatpoint.com/methods-of-information-gathering
12. Nihal Gulammahiyuddin Shaikh, Dhaval Chudasama. Research on Cyber Offenses under Information Technology Act, 2000. Recent Trends in Parallel Computing. 2021; 8(1): 14–20p.

© STM Journals 2021. All Rights Reserved

View publication stats