J. Adv. Res. in Information Technology, Systems and Management
Volume 7, Print Issue 1 - 2023, Pg. No. 1-3
Peer Reviewed Journal

Research Article

Research Paper: Recon for Me

Sanyam Kakkar

Department Of Computer Science & Engineering, Chandigarh University, Gharuan, India.

I N F O

E-mail Id:
19BCS3037@gmail.com
Orcid Id:
https://orcid.org/0009-0006-8564-0235
How to cite this article:
Kakkar S. Research Paper: Recon for Me. *J Adv Res Info Tech Sys Mgmt* 2023; 7(1): 1-3.

Date of Submission: 2023-03-12
Date of Acceptance: 2023-04-29

A B S T R A C T

Getting to know the target system and acquiring information are the first steps in ethical hacking. The term "reconnaissance" refers to a collection of procedures and methods used to acquire and surreptitiously learn as much as possible about a target system, including enumeration, scanning, and foot printing. To find and steal sensitive information, reconnaissance is a crucial step. Attackers would have access to specific information during a proper recon. In this way, penetration testing in information security uses reconnaissance. An attacker utilises recon to communicate with the network's open ports, active services, etc. to gather information without actively using the network. Accessing networks outside of the internet can be made easier with the information it offers. In essence, recon is a gold mine of important information that is vulnerable to intrusion.

Keywords: Information, Reconnaissance, Internet, Recon, Intrusion

Introduction

During reconnaissance, an ethical hacker follows these seven stages to learn as much as they can about a target system:

1. Collecting initial information
2. Determining the network's range
3. Identifying active machines
4. Discovering available access points and ports
5. Identifying the operating system by its fingerprint
6. Locating services on ports
7. Creating a network map

The following actions will be taken by an attacker in order to learn more about a network:

1. File permissions
2. Running network services
3. OS platform
4. Trust relationships
5. User account information

Active and passive reconnaissance are the two basic categories of reconnaissance. Let's examine the distinctions between active and passive reconnaissance.[1-3]

Active Reconnaissance

Cybercriminals that engage in active reconnaissance employ techniques like ping, netcat, automated scanning, and manual testing to try and learn more about computer systems. Active reconnaissance is typically faster and more precise since it generates more noise within the system and has a larger possibility of being detected.[4]

Port Scanning

Port scanning is an example of active reconnaissance. Port scanning is the process of scanning computer ports to identify open ports to a computer since the entire information is going in and out through these ports.

Attackers can find out what services are available and where they can launch an assault by using port scanning. Data is retrieved from open ports and analysed as part of port scanning.[5]

Significance of the Study

Protecting your computers, laptops, servers, smartphones, other electronic devices, network, software, and system data from malicious assaults and other cyberthreats is the practise of cyber security. The use of computers and smartphones has expanded during the last ten years. The internet and smart devices are now a necessary component of everything you do. The internet and the invention of cyberspace are the greatest inventions since sliced bread, but the devil is in the details. Cyber-attacks are on the rise with the growing use of internet in the technologically driven world. The hackers and cyber criminals are shrewd enough to identify loopholes in your cyber security measures and launch cyber-attacks. Therefore, you should always have the top cyber security measures in place to ensure that you are safe while being online. Your data is both your most important and most vulnerable asset in this digital age. Your emails, internet transactions, personal information, and financial information are all highly important pieces of data that cybercriminals are attempting to exploit.

Methodology

Collect all subdomains from tools like subfinder, amass, crtfinder, sublist3r (Use more than tool)

Use Google dorks for example site:ibm.com -www

collect all these informations from subdinder + amass + crtfinder + sublist3r + google_dorks and collect all of them into one text file all_subdomains.txt

[*] Now we have 1 text file contains all subdomains all_subdomains.txt, let's continue…

Pass the text file over httpx or httprobe , these tools will filter all subdomains and return only live subdomains which works on ports 80 and 443

take these live subdomains and collect them into separate file live_subdomains.txt

[*] Now we have 2 text files all_subdomains.txt + live_subdomains.txt

take the live_subdomains.txt file and pass it over waybackurls tool to collect all links which related to all live subdomains

collect all these links into new file waybackurls.txt

[*] Now we have 3 text files all_subdomains.txt + live_subdomains.txt+ waybackurls.txt

take all subdomains text file and pass it over dirsearch or ffuf to discover all hidden directories like https://community.ibm.com/database_conf.txt

collect and filter all the results to show only 2xx, 3xx, 403 response codes from the tool itself (use -h to know how to filter the results)

collect all these informations into text file hidden_directories.txt and try to discover the leakage data or the forbidden pages and try to bypass them

[*] Now we have 4 text files all_subdomains.txt + live_subdomains.txt + waybackurls.txt + hidden_directories.txt

pass all_subdomains.txt to nmap or masscan to scan all ports and discover open ports + try to brute force this open ports if you see that this ports may be brute forced, use brute-sprayto brute force this credentials

collect all the results into text file nmap_results.txt

[*] Now we have 5 text files all_subdomains.txt + live_subdomains.txt + waybackurls.txt + hidden_directories.txt + nmap_results.txt

use live_subdomains.txt and search for credentials in GitHub by using automated tools like GitHound or by manual search (I'll put pretty reference in the references section)

collect all these information into text file GitHub_search.txt

[*] Now we have 6 text files all_subdomains.txt + live_subdomains.txt + waybackurls.txt + hidden_directories.txt + nmap_results.txt + GitHub_search.txt

use altdns to collect subdomains from subdomains, for example sub.sub.sub.domain.com

As usual :) collect all this info into text file altdns_subdomain.txt

[*] Now we have 7 text files all_subdomains.txt + live_subdomains.txt + waybackurls.txt + hidden_directories.txt + nmap_results.txt + GitHub_search.txt + altdns_subdomain.txt

pass waybackurls.txt file over gf tool and use gf-patterns to filter the links to possible vulnerable links, for example if the link has parameter like ?user_id= so this link may be vulnerable to sqli or idor, if the link has parameter like ?page= so this link may be vulnerable to lfi

collect all this vulnerable links into directory vulnerable_links.txt and into this directory have separated text files for all vulnerable links gf_sqli.txt , gf_idor.txt ,etc

[*] Now we have 7 text files all_subdomains.txt + live_subdomains.txt + waybackurls.txt + hidden_directories.txt + nmap_results.txt + GitHub_search.txt + altdns_subdomain.txt and one directory vulnerable_links.txt

use grep to collect all JS files form waybackurls.txt as cat waybackurls.txt | grep js > js_files.txt

you can analyze these files manually or use automation tools (I recommend manual scan, see references)

save all the results to js_files.txt

[*] Now we have 8 text files all_subdomains.txt + live_

subdomains.txt + waybackurls.txt + hidden_directories.txt + nmap_results.txt + GitHub_search.txt + altdns_subdomain.txt + js_files.txt + one directory vulnerable_links.txt

Conclusion

- Maintain a continuous reconnaissance system
- Do not reserve reconnaissance assets
- Orient yourself toward the reconnaissance objective
- Provide accurate and timely information
- Make sure to have room to maneuver
- Contact and maintain enemy forces
- Develop the situation quickly

References

1. https://intellipaat.com/blog/reconnaissance-in-cyber-security/
2. https://www.bajajallianz.com/blog/cyber-insurance-articles/what-is-the-importance-of-cyber-security.html#
3. https://infosecwriteups.com/simple-recon-methodology-920f5c5936d4
4. https://systemweakness.com/simple-recon-methodology-a9ff080b40c8?gi=c0433abea0be
5. https://infosecwriteups.com/recon-methodology-for-bug-hunting-e623120a7ca6