Passive Reconnaissance

Yingwei Liu

Liberty University

Ethical Hacking

Dr. Allen Harper

**Passive Reconnaissance**

|  |  |
| --- | --- |
| **Part 1: Explore Google Hacking Techniques** | |
| **Step 5** | **Provide a screenshot as directed:** |
| **Step 7** | **Provide a screenshot as directed:** |
| **Step 9** | **Describe the differences as directed?**  *The site syntax did not present the main page of the target.com, the inurl syntax will display the target main page. The link site shows the linking pages inside the target websites. Related site will present all these websites that has similar business model like target. Info sites of target website gives all the contact information of the target’s website.* |
| **Part 2: Experiment with Google’s Advanced Search Operators** | |
| **Step 5** | **Provide a screenshot as directed:**  [**https://www.google.com/search?as\_q=target&as\_epq=&as\_oq=&as\_eq=&as\_nlo=&as\_nhi=&lr=&cr=&as\_qdr=all&as\_sitesearch=&as\_occt=any&safe=images&as\_filetype=&tbs=**](https://www.google.com/search?as_q=target&as_epq=&as_oq=&as_eq=&as_nlo=&as_nhi=&lr=&cr=&as_qdr=all&as_sitesearch=&as_occt=any&safe=images&as_filetype=&tbs=)  **vs**  [**https://www.google.com/search?client=firefox-b-1-e&q=target**](https://www.google.com/search?client=firefox-b-1-e&q=target)**.**  [**https://www.google.com/search?q=site:target.com+intitle:index.of**](https://www.google.com/search?q=site:target.com+intitle:index.of) |
| **Step 6** | **Provide a screenshot for each search, as directed:**  [***https://www.google.com/search?q=site:target.com+ext:xml+|xt:conf+|+ext:cnf+|+ext:reg+|+ext:inf+|+ext:rdp+|+ext:cfg+|+ext:txt+|+ext:ora+|+ext:ini***](https://www.google.com/search?q=site:target.com+ext:xml+|xt:conf+|+ext:cnf+|+ext:reg+|+ext:inf+|+ext:rdp+|+ext:cfg+|+ext:txt+|+ext:ora+|+ext:ini)   1. Search for configuration files:   [***https://www.google.com/search?q=site:target.com+ext:sql+|+ext:dbf+|+ext:mdb***](https://www.google.com/search?q=site:target.com+ext:sql+|+ext:dbf+|+ext:mdb)   1. Search for log files:     ***https://www.google.com/search?q=site:target.com+ext:bkf+|+ext:bkp+|+ext:bak+|+ext:old+|+ ext:backup***   1. Search for backups and old files: |
| *https://www.google.com/search?q=site:target.com+inurl:login*   1. *Search for login pages:*   **https:**[**//w**](http://www.google.com/search?q=site%3Atarget%2Bintext%3A%22sql%2Bsyntax%2Bnear%22%2B)**ww**[**.google.com/search?q=site:target.com+intext:%22sql+syntax+near%22+|+int**](http://www.google.com/search?q=site%3Atarget%2Bintext%3A%22sql%2Bsyntax%2Bnear%22%2B)**ext:%22syntax+error+has+occurred%22+|+intext:%22incorrect+syntax+near%22+|+intext:%22unexpected+end+of+SQL+command%22+|+intext:%22Warning:+mysql\_connect()%22+|+intext:%22Warning:+mysql\_query()%22+|+intext:%22Warning:+pg\_connect()%22**   1. Search for SQL errors:  |  |  | | --- | --- | | **https:**[**//w**](http://www.google.com/search?q=site%3Atarget%2Bext%3Adoc%2B)**ww**[**.google.com/search?q=site:target.com+ext:doc+|+e**](http://www.google.com/search?q=site%3Atarget%2Bext%3Adoc%2B)**xt:docx+|+ext:odt+|+ext:pdf+|+ext:rtf+|+ext:sxw+|+ext:psw+|+ext:ppt+|+ext:pptx+|+ext:pps+|+ext:csv**   1. **Search for publicly exposed documents:**     **https:**[**//w**](http://www.google.com/search?q=site%3Atarget%2Bext%3Aphp%2Bintitle%3Aphpinfo%2B%22published%2Bb)**ww**[**.google.com/search?q=site:target.com+ext:php+intitle:phpinfo+%22published+b**](http://www.google.com/search?q=site%3Atarget%2Bext%3Aphp%2Bintitle%3Aphpinfo%2B%22published%2Bb)**y+the+PHP+Group%22**   1. Search for phpinfo():      |  | | --- | | **Part 3: Explore the WHOIS Database** | | | |
|  | |
| **Step 3** | **Provide a screenshot as directed.** |
|  | |
| **Step 4** | **Provide the date, as directed.** |
| *7/03/2022 18:29:37*   |  |  | | --- | --- | | |  | | --- | | **Part 4: Collect Information with theHarvester** | |   **Step 2 Provide a screenshot as directed.** | |
| **Step 4** | **Provide a screenshot as directed.**  *theHarvester -d target.com -b google* |
| **Step 6** | **Provide a screenshot as directed.** |
| **Step 8** | **Provide a screenshot as directed.**    **tells theHarvester program to search through of a Target search on LinkedIn.** |
| *List 300 results from all the source and saved in the test file.*   |  |  | | --- | --- | | |  | | --- | | **Part 5: Collect Information with Maltego** | |   **Step 8 Provide a screenshot as directed.** | |
| **Step 17** | **Provide a screenshot as directed.** |
| |  |  | | --- | --- | | |  | | --- | | **Part 6: Gather Social Engineering Data with LinkedIn** | |   **Step 7 Provide a screenshot as directed.** | |
| **Step 16** | **Provide a screenshot as directed.** |
| |  |  | | --- | --- | | |  | | --- | | **Part 7: Going Deeper** | | | |

Introduction of the Passive Reconnaissance

Passive Reconnaissance is a way to collect and gain information about target.com without actively engaging with the systems. The reason why malicious attackers prefer to use passive reconnaissance is because the target they attacked cannot trace the attacker’s activities and procedures. Even the target that they attacked can secure their internal network and systems with firewall and security policy. But it is hard for the organization to prevent passive reconnaissance since most of the security policy and systems are rely on reactive attack detection and response tools. According to the John Sammons, “a hacker will begin with passive reconnaissance, which doesn’t involve direct interaction, is harder to detect, and doesn’t involve using tools that touch the target’s site, network, or computers.” There are some ways to mitigate and reduce the passive reconnaissance attack. First, improve the security policy and make sure it is updated. Second, the organization need to set up regular security training for employees to aware the potential passive reconnaissance attack.

In order to provide better passive reconnaissance attack, people need to know how to use the google search operator to provide detailed information searching process. The operator that use in the google search to query result from specific domain is *site:* operator. And the operator *link:* will be the search operator allows people to see the links from the target website.

The Google search syntax to search the site exploit-db.com for Firefox exploits is the *Firefox exploits site: exploit-db.com.* People should apply google advance search to increase research’s accuracy. TheHarvester is an effective information gathering tool that allows people to collect organization’s information such as emails, hosts, domains, employee names, etc. Also, the theHarvester integrated with one of the most powerful SHODAN database. According to the Genge, “Shodan has been acknowledged as one of the most popular search engines available today, designed to crawl the Internet and to index discovered services.” TheHarvester -d stands for the domain name of the target and -b allows the user to search specific source.

The Maltego is also an information gathering tool that collect organization’s domain names, network, employee’s email, etc. It is a powerful and efficient information collection tool that allows the user to present the information that they collected into diagram and graph. The graphical view provides direct message to the user and allows them to have better understanding of the information they collected.

When people try to collect employee’s information through LinkedIn, people might view some people information as LinkedIn Member. If people want to view the full information about the user, the best way is to copy the job title of the target, search it in the <https://www.recruitin.net> with LinkedIn. Once it generates a query for the target, it can start search the query on the google and present the search results.

Passive Reconnaissance attack is a way for malicious attacker to gather organizations or individual’s information. In today’s world, the most critical component is the private information and data. As a Christian, people need to respect other’s privacy and do not gather information for malicious purposes. Just like Matthew 5:38-39, “You have heard that it was said, ‘Eye for eye, and tooth for tooth. But I tell you, do not resist an evil person. If anyone slaps you on the right cheek, turn to them the other cheek also.”

From this lab, there are various tools that can apply into the passive reconnaissance. Like how to use TheHarvester and Maltego to collect and present information. Also, people can view private account on LinkedIn through online.

Favorite part of this lab is the practical lab practice. Because it allows people to practice how to defend and use these tools in passive reconnaissance.

The part that I have issues with is the google advanced search part.

I would add more information that how to use Maltego.

References

Genge, B., & EnAchescu, C. (2016). ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services.*Security and Communication Networks, 9*(15), 2696-2714. <https://doi.org/10.1002/sec.1262>.

Sammons, J., & Cross, Michael. (2017). Cybercrime. *The Basics of Cyber Safety,* Retrieved fr <https://www.sciencedirect.com/science/article/pii/B978012416650900005Xom>.

Bible. Matthew 5:38-39.