Lab 03 – Open Source Intelligence Gathering

In this lab, you will work on passive discovery; the first step followed when performing a penetration test. You will explore several passive tools to help discover valuable information about a target organization.

Please remember there is a significant difference between passive and active discovery techniques. Active techniques require prior approval and permission from the target organization. **DO NOT PERFORM active techniques** on a target for which you do not have permission, preferably written within a contract.

Complete the following tasks:

TASK ONE: Passive Discovery

1. Gathering Open Source Intelligence (OSINT) from public resources is extremely valuable when targeting a specific organization from an offensive security standpoint. We are looking for information that can better prepare us to engage our target.

    a) Public information that can be gathered includes, but is not limited to:

    - ✓ Email addresses or even the email structure – one example may be where an organization uses firstname.lastname@company.com.
    - ✓ Passwords – check password breach sites or github for passwords included within software development projects.
    - ✓ Technology publicized and used by the target organization which might be encountered externally or internally to the organization.
    - ✓ Keywords that may help develop a tailored password list which may be used for active techniques such as brute-force attacks.
    - ✓ There are several ideas – the ones listed above are just a small subset.

    This information may help with various technical aspects; however, this may help with social engineering – if the penetration testing engagement requires it. Some will, some will not.

    Select a target organization, such as your employer and perform the following passive discovery tasks; however, please make sure you have prior approval before proceeding. Even though this is a passive discovery, your organization should be aware that you are pursuing this. If you have any doubts, or concerns about pursuing these activities, please use Marist as the target organization.

    Create a profile of your target, such as technologies, ip addresses and ranges, and services.

    b) You should have already downloaded kali linux. Spin up a virtual machine (VM) within your hypervisor, such as VMware Workstation, VMware Fusion, Parallels, or Oracle VirtualBox.

c) Use five passive discovery tools within kali linux to gather intelligence on the target organization. Use the following three tools and you may select two additional tools to use:

- ✓ Recon-ng
- ✓ The Harvester
- ✓ Shodan.io
- ✓ Two Passive Discovery Tools of your choice

d) For each passive discovery tool you execute, provide the following within your report:

- ✓ Screenshots of the tool in use and the results generated.
- ✓ What were the results? Document these as if you were writing a passive discovery report for a customer.
- ✓ Did you find anything surprising? Or, was everything as you expected?
- ✓ What value will you gain from this tool or source of intelligence? How could this intelligence be leveraged for pursuing an active discovery in a penetration test?

For the overall report, discuss how valuable OSINT is and what recommendations you would make to the organization to better protect its resources, data, and information that is publicly available.

TASK TWO: OSINT Literature Review

1. Academic Research:

a) Research Open Source Intelligence Gathering. This may be techniques, tools, or simply theoretical perspectives.

b) Utilize the Marist online library to research and find at least three academic resources, such as: conference papers or journal articles (ie: ACM Digital Library, or IEEE). You may also use google scholar if you wish.

c) You may use additional internet articles after you find at least three academic resources.

d) Write a brief two-page literature review on what you find. You may use APA 7th style formatting or another formatting style of your choice.

e) You may want to sign up for a free Mendeley account to help keep track of your sources. The Mendeley plugin for Microsoft Word works well for resource inclusion and citations; however, you must ensure that Mendeley has the proper information in the proper place for the automatic reference feature to work correctly. Take the time to ensure the formatting is correct.

DELIVERABLE:

1. Complete a professional write-up and include the following information:

    a. **Description:** Brief description, such as an executive summary, depicting an overall view of what topic or technology you are concentrating on within this lab. Keep this short and to the point. Think like a consultant and be mindful that what you are providing should represent you as a professional in the industry.

    b. **Topology/Diagram:** Use Microsoft Visio, or Lucid Chart, to create an aesthetically pleasing network topology or graphical representation depicting an overall view of what you're working on. This may include the source, the target organization, various tools, websites your visiting, IP Addresses, domain names/information, credential used, and anything else you feel would be beneficial to add.

    c. **Key Syntax:** Sometimes it's nice to include key syntax used. For instance, if you're not a Linux guru, it might be nice to include how you configured a static IP Address in the Linux CLI, or what files you needed to modify in order to configure a primary DNS server IP Address or domain suffix. This is especially useful for tools that you may only use once in a while.

    d. **Verification:** Provide key screenshots that display verification that all tasks and all steps of the lab have been completed. For instance, if you used a specific tool, ensure that the reader knows the syntax you used to execute the tool and the intelligence gathered from the tool. Make sure you provide a description of what the screenshot is showing. Do not simply add the screenshot and state, "here is the screenshot". These descriptions and screenshots should paint a story of the work you put into this lab and verify you have successfully completed the virtual environment configuration. Be thorough and professional! A few things to focus on would be:

        i. Screenshots and tables documenting the intelligence you gathered.

        ii. Think of this report as a professional document that you would be handing to a customer (or provided to management for an organization you work for).

    e. **Conclusion:** Wrap up your lab report with a short conclusion. If something did not work, state it. If everything did work successfully, state that as well.

    f. **References:** Make sure you include any works cited here as well as throughout your lab report. If you looked something up, include it.

2. Research the topic presented in task two. Utilizing at least three academic resources, such as conference papers or journal articles found within the Marist online library (ie: ACM Digital Library, or IEEE) or google scholar, write a brief two-page APA 6th-style summary on what you

found (Please do not include a cover page though). You may use additional internet articles after you have found the three academic resources. You may want to sign up for a free Mendeley account to help keep track of your sources. You may use the Mendeley plugin for Microsoft Word; however, you must ensure that Mendeley has the proper information in the proper place for the automatic reference feature to work correctly.

3. Upload the following file(s) to the assignment within iLearn:
   a) A .pdf file of your passive discovery report.
   b) A .pdf file of your research paper.

Good Luck with your lab!