Lab 04 – Scanning the Target for Vulnerabilities

In this lab, you will work on active discovery; the second step followed when performing a penetration test. You will explore several active 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. Also, DO NOT PERFORM ACTIVE TECHNIQUES ON THE MARIST NETWORK OR ANY OTHER NETWORK without prior permission!!!

Complete the following tasks:

TASK ONE: Active Discovery

1. Actively scanning a target organization/network can be a thrilling experience and 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 and potentially move into exploiting a vulnerability that we find.

    a) The following VMs should be downloaded, installed and running within your hypervisor of choice:

    ✓ Kali Linux VM – this will be known as your Attack VM
    → https://www.kali.org/get-kali/

    ✓ Metasploitable VM – this will be known as your Target VM
    → https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

    b) Once you have your VMs downloaded and installed within your hypervisor, it is a good idea to isolate them from your LAN (ie: the network your desktop computer belongs to). Create another network on its own vmnet. In other words, if you have the IP Address of 192.168.1.100/24 on your desktop, then your LAN subnet network address is 192.168.1.0/24. You should configure your Kali Linux VM and your Metasploitable VM on a different subnet such as 192.168.156.0/24.

    c) Use five active discovery tools within kali linux to actively discover services and potentially discover vulnerabilities on the Metasploitable VM.

    ✓ Use nmap, or a similar scanning tool, to scan the Metasploitable VM. Make sure "banner grabbing" is enabled to help find vulnerable services. Explore other scan options as well. Be creative! As you use the tool, capture the syntax you used as well as the output discovered. Answer the following questions:
        i. What scans did you use?

© 2002-2022 Robert M. Cannistra
All Rights Reserved.

ii. What were their results?
iii. Enumerate your top five services that you would target in the next phase of your pentest and explain why you chose these five.

- ✓ Install OpenVAS, Nessus, or Nexpose and perform a vulnerability scan on the Metasploitable VM. As you use the tool, capture the syntax you used as well as the output discovered. Answer the following question:
  i. Do any of your targeted services contain exploitable vulnerabilities?

- ✓ Research and use three other Active Discovery Tools of your choice. As you use the tool, capture the syntax you used as well as the output discovered. Answer the following questions:
  i. Why did you choose this particular tool?
  ii. What were the results?
  iii. What features of this tool were best?

d) [OPTIONAL] For those of you who would like to take this one step further, complete the following:

- ✓ Using a vulnerable service that you identified in the previous steps, search for a module in Metasploit that corresponds to the vulnerable software. Once you have identified this, configure a payload and get a reverse shell on the Target VM (ie: the Metasploitable VM). As you use the tool, capture the syntax you used as well as the output discovered. Answer the following question:
  i. Do any of your targeted services contain exploitable vulnerabilities?

e) For each active 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 active 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 exploiting a vulnerability during a penetration test or as offensive cyber operation?

For the overall report, discuss how valuable the active discovery phase is and what recommendations you would make to the organization to better protect its resources, data, and information.

© 2002-2022 Robert M. Cannistra
All Rights Reserved.

TASK TWO: Active Discovery Use Literature Review

1. Academic Research:

    a) Research Active Discovery (ie: scanning). 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) If you have not done so already, 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. Be specific here.

© 2002-2022 Robert M. Cannistra
All Rights Reserved.

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 during this second phase scan.

    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). Be professional and thorough!

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 or 7th-style summary (or other formatting style of your choice) 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 active discovery report.
    b) A .pdf file of your research paper.

Good Luck with your lab!

© 2002-2022 Robert M. Cannistra
All Rights Reserved.