Lab 4: Scanning for Vulnerabilities

Preliminaries

Refer to Lecture slides in Week 4.

Tasks

Start Win7 VM, Metasploitable2 VM, and Kali VM. Then, complete the following tasks. Write your answers for all questions to your lab report.

1. Start GVM. (Note: Do not run gvm-setup, as we have set it up for you on school VMs.)
   1.1 Use 'gvm-start' command to start GVM. After GVM is started, run the 'sudo ss -antp' command in a terminal. Based on the output of this command, explain which port the GSA daemon is listening on, and attach a screenshot as proof.
   1.2 Change the password of the GSA user 'admin' to be 'admin123'. Write your command line into your lab report, and attach a screenshot to prove that it is executed without errors.
   1.3 What's the URL for Firefox to access the GVM web interface?

2. Create targets under GVM.
   2.1 Create targets for Win7 VM and Metasploitable2 VM respectively. You should choose options according to our lecture slides. Include a screenshot for each target creation into your lab report.
   2.2 Explore the GSA web interface to find out the following:
      a) How many TCP ports will be scanned if the port list 'All IANA assigned TCP' is used?
      b) Will the TCP port '4' be scanned if this port list is used?

3. Scan Win7 VM.
   3.1 Create a task to scan Win7 VM. Name this task 'Win7', and choose 'Full and Fast' for Scan Config. Include a screenshot of the task configuration into your lab report.
   3.2 After the scan is done, download the GVM report in PDF. The report should be saved to the folder '/home/kali/Downloads'. Then, execute 'cd /home/kali/Downloads' and 'ls -l'. Based on the output of 'ls -l', what's the size of your GVM report for Win7 VM?
   3.3 Rename this GVM report to a more meaningful name using the 'mv' command. Write your command line into the lab report.
   3.4 Use Firefox to visit uni email to email this GVM report to you, or you can use other means to transfer this report out of the virtual lab environment. Compare your GVM report for Win7 with the sample one provided to you on vUWS. Focus on the 'Results Overview' section of both reports. According to this section,
      a) How many results of severity 'High' are reported in your report totally?
      b) How many results of severity 'High' are reported in the sample report totally?

4. Scan Metasploitable2 VM.
   4.1 Create a task to scan Metasploitable2 VM. Name this task 'Meta2-Discovery', and choose 'Discovery' as Scan Config. Include a screenshot of the task configuration into your lab report.

4.2 Explore the GSA web interface to find out how many NVTs will be executed under the 'Discovery' Scan Config?

4.3 After the scan is done, download the GVM report in PDF. Then, run 'cd /home/kali/Downloads' and 'ls -l'. Based on the output of 'ls -l', what's the time of your GVM report for Metasploitable2 being saved?

4.4 Rename this GVM report to a more meaningful name using the 'mv' command. Write your command line into the lab report.

4.5 Use Firefox to visit uni email webpage to email this GVM report to you, or you can use other means to transfer this report out of the virtual lab environment. Look at the 'Results Overview' section of this report. According to this section, how many results of severity 'High' are reported totally?

4.6 Create a second task to scan Metasploitable2 VM. Name this task 'Meta2-Full', and choose 'Full and Fast' as Scan Config. Include a screenshot of the task configuration into your lab report.

4.7 Explore the GSA web interface to find out how many NVTs will be executed under the 'Full and Fast' Scan Config?

4.8 After the scan is done, download the GVM report in PDF. Rename this GVM report to a more meaningful name using the 'mv' command. Write your command line into the lab report.

4.9 Use Firefox to visit uni email webpage to email this GVM report to you, or you can use other means to transfer this report out of the virtual lab environment. Look at the 'Results Overview' section of this report. According to this section, how many results of severity 'High' are reported totally?

5. Understand the reports. (Make sure you really spend time to understand them, not just to complete the tasks in this lab.)

5.1 Look at your GVM report for Win7.

a) How many results have severity 'Medium' according to the 'Results Overview' section?
b) In the 'Results per host' section, under the TCP port 445, there should be one result with severity 'High'. What is the name of the NVT that detect this result?
c) Study the details of the result mentioned in b) above. Answer the following questions in your lab report.
   i) What is the solution recommended for this vuln?
   ii) What are the affected OSes listed for this vuln?
   iii) What are the related CVE IDs and BIDs for this vuln?

5.2 Look at your GVM report from task 'Meta2-Full' for Metasploitable2.

a) How many results have severity 'Medium' according to the 'Results Overview' section?
b) Study the details of the result "Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability". What are the summary and the solution listed for this vuln?

Last but very important: First shutdown and then power off all your three VMs. Our school's cloud is under heavy load, as you can see your VMs may not respond to you quickly. Therefore, if you are not using them, you should have them shutdown and power off.