Foundations of Breach & Attack Simulation

Exercise 1: Continuous Security Validation 1. Click on the CREATE NEW ASSESSMENT button 2. Click CHOOSE TEMPLATE. 3. On the Assessment Templates page, click the dropdown under Select template type, and choose Security Controls. 4 4. Find the Content Filtering assessment template on the page, and click it. 5. Click Create New. 6. Add both assets to the Assessment. a. Click the Manage Assets button b. Click the checkboxes of BOTH assets listed. c. Click Apply 5 7. Under the assets, where it lists the tests configured, click on the three dots under the ACTION column for the test name Social Media sites. 8. Click Manage Scenarios. 9. Under the details column, click on the icon to see the details for Test Web access to Social Media site Facebook. 6 10. On the resulting scenario details page for Test Web Access to Social Media Site Facebook, read and make a note of the scenario description. 11. Click on the heading for Scenario Configuration to expand the configuration details. 12. Review the configuration settings and make note of the Headers sent during the test. Also, make a note of the method being used. 13. Return to the assessment page and click Done to close the scenario listing for the Social Media sites test. 14. Click the Continue button in the bottom right-hand corner of the page. 15. Click the Run Now button.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Exercise 2: Continuous Security Validation - Reviewing The Data With the testing from Excercise 1 completed, we can begin to explore the results of the emulation. 1. Note the results in the top three panels for Overall Combined, Overall Prevention, and Overall Detection scores. 2. In the Overall Detection score panel, expand Security Controls to see detection rates for security controls involved in testing. 8 3. Under the Results menu item, click on Summary 4. Scroll down the results page until you find the Scenario results for Test Web access to Social Media site Facebook. 5. Click on the entry for Test Web access to Social Media site Facebook. 9 6. If you’ve forgotten what this scenario is trying to accomplish, click the ? icon next to the scenario title. 7. Expand the Activity Details and make note of the response code received vs. the response code anticipated. 8. Expand the INDICATORS OF COMPROMISE (IOCS) DETAILS a. Make a note of the following information: i. Destination: ii. HTTP Method iii. Protocols iv. Request Path v. Source Port

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Exercise 3: FIN6 Emulation 1. Click on the three horizontal lines in the top left-hand corner of the screen to open the main menu. 2. Click on ASSESSMENT in the main menu. 11 3. Click on the CREATE NEW ASSESSMENT button 4. Click CHOOSE TEMPLATE. 5. On the Assessment Templates page, click the dropdown under Select template type, and choose Threat Emulation.. 12 6. Find the FIN6 assessment template on the page, and click it. 7. Click Create New 8. Add both assets to the Assessment. a. Click the Manage Assets button b. Click the checkboxes of BOTH assets listed. c. Click Apply 13 9. Under the assets, where it lists the tests configured, click on the three dots under the ACTION column for the test name Lateral Movement. 10. Click DELETE TEST. 11. Click OK 12. Click the Continue button in the bottom right-hand corner of the page. 13. Click the Run Now button

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Exercise 4: MITRE ATT&CK Mapping 1. In the left-hand menu, under Results, click on MITRE ATT&CK 2. Review the results for Prevention. 3. Click on the Detection radio button to toggle the view to detection results. 4. Click the Combined radio button to toggle the view to combined detection and prevention results. 5. Click on the Discover tactic column heading. 6. On the Results page you will see a listing of results that have been filtered to display scenarios from the FIN6 assessment that fall under the ATT&CK tactic of Discovery. 15 7. Click on the line item for Get Hardware Model Using WMI (either one is okay). 8. Click the ? icon next to the scenario title and read the scenario description to get a better understanding of what this scenario is trying to accomplish. 9. Make a note of the WMI command used to obtain the hardware model, you will need this information for your final exam. 16 10. Review the Activity Details to see the output or error code for the scenario. 11. Review the Indicators of Compromise (IOCs) Details

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Exercise 5: Reporting 1. Click on FIN6 (Results) in the breadcrumb navigation at the top of the page. 2. Click on Reports in the left-hand menu. 3. Click the ADD Report button. 4. Give your report a name, select MITRE ATT&CK Report as the report type, and chose the assessment you ran in previous exercises. 18 5. Click SAVE CHANGES. 6. Click on the three vertical dots at the end of the row for the report you just created. 7. Click VIEW. 8. Review the report to get a better understanding of how the lab environment responded to different MITRE ATT&CK techniques.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated