CYBS 7355 - Penetration Testing and Vulnerability Assessments Final Exam Spring 2020 NAME: STUDENT ID: 4 Questions Total Instructions: Save your exam with the filename “CYBS 7355 Final Exam - Name”. Once you are finished, post your exam to the Unit 12 submission folder on the BrightSpace website. Review the questions carefully as some are worth more than others. You will want to allocate proper time to complete all of the questions. All questions will be graded for full, half, or no credit. Please limit your responses to two pages per question. I certify that this is my own work and I have cited all work that is not mine by quotes and citation or by paraphrasing with citations using APA. I understand that if I have plagiarized or copied materials that are not my own work that I will fail this exam with a grade of zero and be subject to academic review. This includes cutting and pasting. Do not use endnotes or footnotes as this is not the APA method. NAME: DATE: CYBS 7355 Penetration Testing & Vulnerability Assessments – Final Exam, Spring 2020 Page 2 1. 100 Points - In Lab #5 “Attacking a Vulnerable Web Application and Database” you were able to exploit a web application using both Reflected Cross Site Scripting (XSS) and SQL Injection vulnerabilities that exist within the DVWA. Often web applications are vulnerable to allowing the use of full command line commands from within the web application. You have been tasked with proving this vulnerability exists on a new website the Dev team is rolling out in December. Repeat the steps in Part 1 of Lab #5 to login to the DVWA application. Once you have set the DVWA Security to “Low” and clicked “Submit”, click on the Command Execution button on the left. 1. What account is this web application running under? 2. What is the current directory on the web server? 3. What files are in the current directory? 4. Can you list the processes currently running on the web server? 5. What is the name of the operating system on the remote web server? Provide screenshot proof of all of your work and steps for full credit, including the actual lab desktop (to show date/time). More is better!! (Hint: Remember the basic Linux CLI commands you have used previously!! Also the “&” sign will allow you to bundle commands together, (e.g. ls & pwd). Extra Credit: 10 bonus points if you can show me the contents of the /etc/passwd file on the remote web server (screenshot required) 2. 50 Points – One of the most successful attacks against wireless networks (WLAN) is the Evil Twin attack. The goal is to introduce an attacker-controlled wireless access point near the “known good” WLAN network. This access point will advertise the exact same SSID as the authorized WLAN. Wireless users may accidently connect to this malicious access point thinking it is part of their authorized network. Once the connection is established, the attacker can initiate a man-in-the-middle attack and capture or relay traffic while eavesdropping on the entire communication. Explain the potential risk an Evil Twin attack like this this would present, not in theory, but to your own organization (company, school, etc.) and how you would go about setting up an Evil Twin attack if you were an attacker. Detail the goals, tools, process, and methodology. Use whatever research will assist you. Provide screenshots if possible to demonstrate what you are doing (these can be captured from your own examples or from a 3rd party). Limit your response to 3 pages or less, double spaced. CYBS 7355 Penetration Testing & Vulnerability Assessments – Final Exam, Spring 2020 Page 3

3. 50 Points – Malware – Your cybersecurity team is finally getting a break after dealing with an outbreak of the new malware W32/CoinMiner hit the corporate network, impacting productivity over the holiday weekend. It was determined this was caused by one of the sales folks who clicked on a “get rick quick” link. The attackers were able to use your company’s computing resources to generate a cryptocurrency mining pool, negatively impacting server performance. As your team is headed home for some much needed rest, your manager pulls you aside. “Hey…you’re finishing up your Master’s Degree in Cybersecurity, right? I’d really appreciate it if you could do a little research into this whole CoinMiner mess and write up the Security Incident Report for us. Be sure to add in any relevant technical details you can about the file paths or registry keys it may touch as well. Need that report by Tuesday! Have good night!” Complete a 1-2 page assessment of the W32/CoinMiner malware using the format you used in Unit 10. Be sure to include the specific technical details on the file paths, registry keys, etc. The intent here is that you demonstrate your ability to effectively research and analyze new malware and report up to higher what you have learned. 4. 50 Points – Your CISO sees you in the hallway. “Hey! You did a terrific job helping me sift through all those Advanced Malware Protection vendors that hounded me last month at the security conference. I was hoping you could help one more time. The business is getting ready to roll out a new web application for our new product line, the UltraWidget 4000. They want it up and running for the 2020 holiday season. I am a bit concerned that we’ve not done all that we should to adequately test the web application before it went live. I’ve been hearing a lot of chatter about ‘Web Application Firewalls” and I know they meet the PCI DSS 3.2 requirements. Could you help me identify 2-3 key features we should be looking for and provide me with a couple of vendors and your recommendation for a good WAF? Don’t worry about pricing…..we’ll get the business to pay for it. We just need to pick the best solution to secure the business.” Identify 2-3 key features that a good WAF should have and then identify and research 3 WAF vendors and their products that will meet the needs of your retail business. Provide a detailed Pros/Cons list for each, make your selection and provide justification for your selection. Be very clear and concise (and make it obvious what your choice is!). Keep your total answer to 3 pages or less, double-spaced. You do not need to provide references.