Cybersecurity Autumn 2023
Exercises Compendium

Frederik Busch

October 4, 2023

Student Mail: frbus21@student.sdu.dk
Date: mm/dd/yyyy

Contents

1 Exercise 01: Setting Up the Lab

VMs installed
Networks Set Up

2 Exercise 02: Starting the Journey

2.1 02a: Thinking About Threats

2.1.1 How did they separate access & infrastructure according to data relevance & impact?

2.1.2 How do roles and personnel fit into this, and which role could policiesand training play?

2.2 02b Pentesting intro: Tutorial on Metasploit

2.2.1 Which advantages for penetration testing would you see in the different approaches? What is the best option?

2.2.2 How does inspecting the ip configuration of a system help you with penetrationtesting? What is the security relevant aspect?

2.2.3 How do you get the targeted user to execute our malicious payload?

2.2.4 What is the practical use of this exercise? And why is the payloadworking in the way it is? How does this exercise relate to remote & reverseshells?

2.2.5 As user and the owner of this system – how would you mitigate thisattack?

2.2.6 How does knowing user names help an attacker/penentration tester?

2.2.7 Using the meterpreter shell, check the output of the "arp" command.What do you find? Why could this information be relevant?

2.2.8 Now lets be on the other side of the fence and investigate suspiciousconnections to our metasploitable server.Which command can you use to see network status and connections?Is there an anomaly or suspicious connection to our server? What makesit suspicious?

3 Exercise 03: General Assessment

3.1 Finding information with whois

3.1.1 What do you learn about SDUs network? In the protocol, note the IPrange.

3.1.2 What is the whois information for nextcloud.sdu.dk? What do you observein comparison to the whois-information you gathered for www.sdu.dk.

3.2 Question: nmap

3.2.1 Send packets with specified ip options

3.2.2 Spoof your MAC address

3.3 Comparing the Tools

3.3.1 Compare your results from each of the previous activities in each question (e.g., sparta vs nessus vs openvas). Take notes & discuss overlaps and differences inresults, pros and cons, ease of use for each tool.

3.4 Collecting the Assessment Information

3.4.1 Service, port number and version number, e.g., FTP 21 vxxxx

3.4.2 Describe or explain at least one vulnerability that you found for thatservice, i.e., what is the underlying issue and what can be achieved?How severe is that issue? (You do not have to state how to exploit thevulnerability or go into technical details. We will look into this later btw.the intricate technicalities are mostly outside the scope of the course.) Butmake sure you describe what possible outcomes of the exploit are, whatthe impact for a real system were and how criticial you would assess theissue due to the effects, i.e., argue for your assessment.

3.4.3 For each of the vulnerabilities in the previous point, note the CVE and/orSource of information about the vulnerability for that version. Usingmetasploits info command might help you here, if you want to go to thecommand line.

3.5 Completing the Assessment

3.5.1 Create a final report, extending the collected information with an overall reviewof the security concerns in both the Metasploitable-3 Windows and Ubuntusystems, e.g., different criticality levels of the services (an overview of how badthe situation is) and which ones to to be prioritized when addressing securityissues (a selection of the most relevant issues for prioritisation). For this use acombination of the results from the tools that you used or one of the tools.

4 Exercise 04: SQL Injection

4.1 SQL Injection

4.1.1 Does it mean the MySQL server is protected against cyber attacks? From Kali,try:mysql -h ¡METASPLOITABLE IP¿ -P 3306

4.1.2 How could that protection look like?

4.1.3 And what exactly would it protect against?

4.2 Spying with SQL Injection

4.2.1 Please shortly discuss your opinion of this web servers configurationconcerning directly listings.

4.2.2 What type of SQLi attack works? Can you explain why?

4.2.3 What is the # sign for? Can we generally assume it to do the trick?

4.2.4 Include four relevant username/password combinations in your report.What is the issue with the passwords in the data base and what could bedone to secure them?

4.2.5 Which other problem allows you to get into the machine using ssh? Howcould this be prevented?

4.3 Elevation of Privilege

4.3.1 Which are the individual issues that allowed us to go from a web interfaceto root access, and how would you address them as a servers operator toprevent them being exploited? Describe the issues you identified and tryto come up with suggestions on how to fix them.

4.3.2 Can SQL Injection expose an otherwise inaccessible data base server?

4.3.3 How likely do you think an attack scenario as presented here is?

4.4 Using our Foot in the Door for Access to Other Services

4.4.1 Is sudo necessary? What do we gain by using it?

4.4.2 Are there other ways to search for a file? Which do you know?

4.4.3 What was the problem with the web application?

4.4.4 Which ports and services were the problem associated with?

4.4.5 How did you exploit the vulnerability?

4.4.6 And what were you able to do?

4.4.7 How would you suggest to fix the problem? (Do some online research aboutSQL injections solutions.)

4.4.8 Draft a shortly and crisply, the relevant parts of a policy trying to prevent theseissues.

text

4.5 Fully Explore Local Accounts

4.5.1 What are benefits of performing this scan after already having full access?

4.6 Post-Exploitation

4.6.1 Thinking as an attacker, what would your next steps be?

4.6.2 As an operator, what would you do to counteract?

4.7 Obfuscated Malware

4.7.1 Task 1 - Take your time to look at the code. Is it readable?

4.7.2 Task 3 - What does the code do? Is it a malicious software and if so how wouldyou classify it?

5 Exercise 05: Drupal

5.1 Background

5.1.1 Which vulnerabilities do you think can be used? Pick two potential vulnerabilitiesand describe them in terms of why you picked them, i.e., date and exploit effect.

5.1.2 For the rest of the tutorial, we will use the vulnerability dubbeddrupageddon.What is the underlying vulnerability?

5.1.3 What is so severe about the issue?

5.2 Post-Exploitation

5.2.1 What are possible activities/aims for the post-exploitation phase?

5.2.2 Write out the list in the file that has the "User Accounts"?

5.2.3 How does having a list of user names help?

5.2.4 What do the excellent post exploitation scripts for linux offer?

5.3 Reflection

5.3.1 What is the main issue with the web server? How did it help selecting potentialexploits?

5.3.2 When opening the drupal web page, you are greeted by a warning. Do you thinkthis is good practice? Why or why not?

5.3.3 Given a more restrictive web server configuration, finding the relevant information wouldnt have been that easy. Please check dirbuster, to be found in the "Web Appli-cation Analysis" menu. How could this tool help you finding information? Try it outon the Ubuntu metasploitable VM. Use/ usr/ share/ dirbuster/ wordlists/ directory-list-2.3-medium.txtas dictionary.

5.3.4 How can effective spying with tools likedirbusterbe prevented?

5.3.5 This attack didnt get us all the way to root. How would you continue the pentest?What would be your next actions?

5.3.6 Do you have any specific things in mind you would try to get root access?

5.3.7 What makes getting a remote shell so powerful?