Network Security Logbook

Student:

Alessandro BUONERBA

Module Leader:

Dr Anatolij BEZEMSKIJ

Computer Science (Cybersecurity)
Network Security
COMP-1829

Department of Computing & Mathematical Sciences
Liberal Arts & Sciences

University of Greenwich
London, United Kingdom

December 2021

CONTENTS

LIST OF FIGURES

1

WEEK 1: NETWORKING QUIZ

In the first week, there was no laboratory but an introduction to Networking with explanations of the various parts that led to Network Security. At the end of the lecture, we had access to a Quiz. My results are below.

Summary of your previous attempts

Attempt	State	Grade / 19.00	Review
1	Finished Submitted Wednesday, 29 September 2021, 12:42 PM	17.00	Review
2	Finished Submitted Wednesday, 29 September 2021, 12:47 PM	18.00	Review

Your final grade for this quiz is 18.00/19.00.

Figure 1.1: Networking Quiz Results

WEEK 2: MALWARE

There are several types of Malware that can be used to compromise a network or a computer.The propagation of a malware can also happen through social engineering, being phishing one of the most common examples (Greenberg, 2019). This lab objective is to discover and research different types of specific malwares.

2.1 ZEUS GAMEOVER

One of the most famous malware is Zeus Gameover. Zeus is a trojan that spreads itself through emails with malicious attachments (Wikipedia, 2021). This malware will then generate zombies that sit in an IRC server managed by a server administrator. This process is a continue and infinite loop and makes the battle against the botnets really hard (Firat, 2020). Zeus uses anAdobe Reader BMP/RLE heap corruption vulnerability CVE-2013-2729 that causes a buffer overflow to cause a DoS that makes the daemon crash and execute malicious code (Ismail et al., 2021). In the case of Zeus, most of the time, a PDF file is used to initialise everything and start the new botnet. It will use the vulnerabilities of the reader to declare previously where the shellcode is not even hidden, and that can be easily decrypted (Eternal, 2013). These discoveries are made using a python tool named peepdf that analyse a pdf file. The principal scope of the botnet is to steal banking informations where the victims are deprived of their money when the amount is worth to be taken (KnowBe4, 2020).

Figure 2.1: Shellcode Zeus Gameover

3

WEEK 3: DENIAL OF SERVICE

Where all Week 3 stuff will go

4

WEEK 4: CYBER PHYSICAL ATTACKS

Where all week 4 stuff will go

WEEK 5: WEB SECURITY

Where all week 5 stuff will go

6

WEEK 6: SOCIAL ENGINEERING & PHISHING

Where all week 6 stuff will go

7

WEEK 7: CLOUD, BYOD AND INSIDER THREAT

Where all week 7 stuff will go

8

WEEK 8: DEFENCE MEASURES

This is where all week 8 stuff goes.

9

CONCLUSION

This is the conclusion.

BIBLIOGRAPHY

Eternal, Todo (Jan. 2013). *Spammed CVE-2013-2729 PDF Exploit Dropping ZeuS-P2P/Gameover | Eternal-Todo.Com*. URL: https://eternal-todo.com/blog/cve-2013-2729-exploit-zeusp2p-gameover (visited on 10/06/2021).

Firat, Ibrahim (2020). *Inevitable Battle Against Botnets*. Hershey, PA: Information Science Reference, an imprint of IGI Global. ISBN: 978-1-79985-348-0.

Greenberg, Andy (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. First edition. New York: Doubleday. ISBN: 978-0-385-54440-5 978-0-525-56463-8.

Ismail, Zahian, Aman Jantan, Mohd. Najwadi Yusoff, and Muhammad Ubale Kiru (Mar. 2021). "The Effects of Feature Selection on the Classification of Encrypted Botnet". In: *Journal of Computer Virology and Hacking Techniques* 17.1, pp. 61–74. ISSN: 2263-8733. DOI: 10.1007/s11416-020-00367-7. URL: https://doi.org/10.1007/s11416-020-00367-7 (visited on 10/06/2021).

KnowBe4 (Nov. 2020). *Gameover Zeus (GOZ) | KnowBe4*. URL: https://www.knowbe4.com/gameover-zeus (visited on 10/06/2021).

Wikipedia (June 2021). "Gameover ZeuS". In: *Wikipedia*. URL: https://en.wikipedia.org/w/index.php?title=Gameover_ZeuS&oldid=1030426212 (visited on 10/06/2021).