Tilastotieteen harjoitustyö 2021

Harjoitustyö TILM3558

2.12.2021

Marko Järvinen – 518467

Table of Contents

[1 Introduction 3](#_Toc89381210)

[2 References 4](#_Toc89381211)

[Appendices 6](#_Toc89381212)

[Appendix 1 Meeting minutes (assignment 4) 6](#_Toc89381213)

# Introduction

# References

|  |  |
| --- | --- |
| [1] | Kaspersky, "Cyberthreat Real-Time Map," [Online]. Available: https://cybermap.kaspersky.com/. [Accessed 15 9 2021]. |
| [2] | Microsoft, "The evolution of malware and the threat landscape - a 10-year review," 2012. |
| [3] | Microsoft, "Digital Defense Report," 2021. |
| [4] | E. Paul, "EMP Trust HR," 12 9 2017. [Online]. Available: https://www.emptrust.com/blog/benefits-of-using-digital-signatures. [Accessed 22 9 2021]. |
| [5] | Microsoft, "Microsoft Docs," 2 4 2021. [Online]. Available: https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image\_optional\_header32. [Accessed 22 9 2021]. |
| [6] | M. Vanhoef, "Key Reinstallation Attacks," [Online]. Available: https://www.krackattacks.com/. [Accessed 29 9 2021]. |
| [7] | Computerphile, "Krack Attacks (WiFi WPA2 Vulnerability)," 18 10 2017. [Online]. Available: https://www.youtube.com/watch?v=mYtvjijATa4. [Accessed 29 9 2021]. |
| [8] | Wi-Fi Alliance, "Discover Wi-Fi - Security," [Online]. Available: https://www.wi-fi.org/discover-wi-fi/security. [Accessed 29 9 2021]. |
| [9] | darkAudax, "Tutorial: Simple WEP Crack," 11 1 2010. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=simple\_wep\_crack. [Accessed 29 9 2021]. |
| [10] | Wireshark, "How to Decrypt 802.11," 1 4 2020. [Online]. Available: https://wiki.wireshark.org/HowToDecrypt802.11. [Accessed 29 9 2021]. |
| [11] | Kaspersky, "What Is an Advanced Persistent Threat (APT)?," [Online]. Available: https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats. [Accessed 4 10 2021]. |
| [12] | Wikipedia, "GhostNet," [Online]. Available: https://en.wikipedia.org/wiki/GhostNet. [Accessed 4 10 2021]. |
| [13] | Trend Micro, "Targeted Attacks," [Online]. Available: https://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks. [Accessed 4 10 2021]. |
| [14] | Symantec, "Symantec Internet Security Threat Report," 2006. |
| [15] | Owasp, "Session hijacking attack," [Online]. Available: https://owasp.org/www-community/attacks/Session\_hijacking\_attack. [Accessed 4 10 2021]. |
| [16] | M. Ayoub, "Session attacks and defense methods," 26 4 2012. [Online]. Available: https://medium.com/@mena.meseha/session-attacks-and-defense-methods-97afa42e27f9. [Accessed 4 10 2021]. |
| [17] | Webopedia, "Input Sanitazion," 23 6 2021. [Online]. Available: https://www.webopedia.com/definitions/input-sanitization/. [Accessed 4 10 2021]. |
| [18] | A. Koivu, L. Koivunen, S. Hosseinzadeh, S. Laurén, S. Hyrynsalmi, S. Rauti and V. Leppänen, "Software Security Considerations for IoT," in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2016. |
| [19] | Microsoft, "Microsoft Docs," 7 1 2021. [Online]. Available: https://docs.microsoft.com/en-us/windows/win32/memory/data-execution-prevention. [Accessed 17 10 2021]. |
| [20] | Micro Focus, "Data Execution Prevention," [Online]. Available: https://www.microfocus.com/documentation/extend-acucobol/1001/GUID-7ED0BF06-1331-4CDF-A887-98B4F2DB8306.html. [Accessed 17 10 2021]. |
| [21] | Wikipedia, "Return-oriented programming," [Online]. Available: https://en.wikipedia.org/wiki/Return-oriented\_programming. [Accessed 18 10 2021]. |
| [22] | A. Verma, "Production honeypots: An organization’s view," *SANS Security Essentials,* 2003. |
| [23] | Wikipedia, "WannaCry ransomware attack," [Online]. Available: https://en.wikipedia.org/wiki/WannaCry\_ransomware\_attack. [Accessed 18 10 2021]. |
| [24] | V. Leppänen, S. Rauti, K. Rindell and J. Holvitie, "CYBER SECURITY AND SECURING DATA," 6Aika, 2020. |

# Appendices

## Appendix 1 Meeting minutes (assignment 4)

**MEETING MINUTES**

**Groupwork assignment 4**

**Place:**

Discord voice call

**Date and time:**

30.9.2021 10:00

**Chairperson:**

Marko Järvinen

**Present:**

* Marko Järvinen
* Elmeri Selänne
* Roope Pouta
* Jesse Järvi
* Tomas Kopra

**Not present:** -

**Summary of meeting participation after this meeting:**

No one has missed a single meeting.

**Chairperson opened the meeting at 10:00**

**Notes:**

* F-secure does not seem to have any good info about APTs.
* APTs are long duration targeted attacks against big corporations and governments.
* Injecting <img/> tags to the website was funny.
* We can't seem to figure out what the attack on a) is called. We will call it identity theft, for now.
* To prevent attacks like a) proper authentication measures should be taken.
* Attack on b) is HTML injection.
* To prevent attacks like b), the website developer should implement data validation on their inputs.
* Attack on c) seems to be called cross site request forgery.
* Alerting the user's session id works by injecting a <script> tag into the input field and running some JavaScript in it which fetches the correct cookie (PHPSESSID) from the browser cookies.
* Our injected JavaScript POST requests do not seem to work.
* Attacks like c) can also be prevented by proper input validation.
* Some challenges in securing IoT devices are, for example, the need to be able to control many devices at once wirelessly. This leads to them having similar security measures and cracking one device makes it possible to crack the other devices as well.
* Hardware limitations pose a challenge in securing IoT devices (not enough space for proper encryption methods, for example).

**Chairperson closed the meeting at 12:01**