TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Andrei Aleksejev 201756IVSB

SECURITY EVALUATION AND TESTING OF SOFTWARE FOR HOME SERVER

Bachelor's Thesis

Supervisor: Edmund Laugasson
Master degree

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Andrei Aleksejev 201756IVSB

KODUSERVERI TARKVARA TURBE HINDAMINE JA TESTIMINE

Bakalaureusetöö

Juhendaja: Edmund Laugasson
Master degree

Tallinn 2023

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: Andrei Aleksejev

15.05.2023

Abstract

The aim of current thesis is to test security related configurations for application installed and served by home server and evaluate security of server. To choose configurations for testing official documentation and guides for security hardening, provided by software developer, is used.

Thesis contains multiple experiments to evaluate and test every configuration separately. To perform experiments and tests an environment created with help of virtualization software, that resembles real server set up as close as possible. To create testing environment official documentation is used.

The emphasis of this thesis work is security and finding out, what kind of effect configurations have on security of server created in testing environment. Result is evaluation of configurations and their effectiveness in terms of server security.

The thesis is written in English and is 41 pages long, including 8 chapters, 1 table.

Annotatsioon

Koduserveri tarkvara turbe hindamine ja testimine

Käesoleva lõputöö eesmärk on testida koduserveri installitud ja teenindatud rakenduste turvalisusega seotud konfiguratsioone ning hinnata serveri turvalisust. Konfiguratsioonide valimiseks ametliku dokumentatsiooni testimiseks ja tarkvaraarendaja poolt pakutavaid turvalisuse kõvenemise juhendeid kasutatakse.

Lõputöö sisaldab mitut katset, et hinnata ja testida iga konfiguratsiooni eraldi. Katsete tegemiseks ja testimiseks virtualiseerimistarkvara abil loodud keskkond, mis sarnaneb võimalikult lähedale loodud reaalsele serverile. Testimiskeskkonna loomiseks kasutatakse ametlikku dokumentatsiooni.

Selle töö rõhk on turvalisusel ja välja selgitamisel, millist mõju avaldavad konfiguratsioonid testimiskeskkonnas loodud serveri turvalisusele. Tulemuseks on konfiguratsioonide ja nende tõhususe hindamine serveri turvalisuse seisukohast.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 41 leheküljel, 8 peatükki, 1 tabel.

List of Abbreviations and Terms

CA	Certificate Authority
DB	Database
DNS	Domain Name System
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
LTS	Long-Term support
MITM	Man-in-the-middle attack
OS	Operating System
OWASP	Open Worldwide Application Security Project
RDBMS	Relational Database Management System
SSL	Secure Socket Layer
SQL	Structured Query Language
UFW	Uncomplicated Firewall
UI	User Interface
URL	Uniform Resource Locator
VM	Virtual Machine
WebDAV	Web Distributed Authoring and Versioning
2FA	Two Factor Authentication

Table of Contents

1. Introduction

Setting up home server to provide different services for personal use is a common thing nowadays. A home server is a computer system that is used to store and manage data, host applications, and provide services such as file sharing and media streaming. With the increasing amount of data generated by households and small businesses, home servers have become an affordable and convenient solution for managing and accessing this data. As any other system home server requires careful attention from a person to use a sufficient security measure to minimize possible risks, as it potentially exposes private and personal data to external threats and intruders. This is the reason, why in author's opinion topic of this thesis work has high actuality.

This thesis aim is to evaluate security level of certain software that can be used for home server solutions. It will examine different configuration options for possible combination of OS and software for home server solutions. As this work is limited in volume it is not possible to cover every possibility, so a specific set of software will be tested.

The research for this thesis will be conducted through a practical experimentation. Various configurations will be used for software that is installed on server and tested to determine, what kind of impact different options have on security and amount of vulnerabilities that can be exploited to get unauthorized access to server. A certain criteria will be determined to conduct experiments in methodology section of this thesis work. Based on this criteria evaluation of impact on server security connected to change in configurations of software will be performed.

To perform experiment part of this thesis work an environment will be set with help of virtual machines. There will be at least two machines to conduct practical part: one machine will be used to host home server and provide access to service for user, second machine will be used to perform penetration testing of service provided by first machine. More detailed description and requirements of environment will be provided in methodology part of this thesis.

For testing purposes tools, that are best suited for each testing scenario, will be used to ensure accurate results and decrease possibility of mistakes and other inaccuracies during penetration testing phase of practical part of this work. Main aim of using penetration testing tools will be to find and if possible exploit available vulnerabilities.

The findings of this thesis will be of interest to individuals considering the use of a home server for managing, accessing their data and providing services for personal use. It will also provide example to possible server set-up and ways to test individual's system for vulnerabilities and what kind of tools required to perform such testing. Main goal is to highlight importance of sufficient configuration of services and OS to ensure high security level of system and maintain integrity of individual's data stored on server. Additionally, the research may contribute to the broader discussion on the benefits and challenges of decentralized data management and the role of home servers in this context.

2. Methodology

2.1 Methodology overview

The purpose of this chapter is to describe the methodology used during experiment process conducted as part of this thesis. The methodology includes the research design, configuration selection, software choice, data collection, and data analysis procedure.

The research design used for this thesis work is an experiment. This design was chosen because it suits best and allows for manipulation of configuration of software that is used on server during experiments. More precisely, the experiments conducted in this thesis are aimed to evaluate, what kind of impact on security and available vulnerabilities that can be exploited, and how effective are available security related configurations.

Security evaluation methods. There exists several methods for evaluation of system security.[1]

Penetration testing: This is a method of evaluating the security of a system by simulating an attack on it. It involves attempting to exploit vulnerabilities in the system to gain access to sensitive information or functionality.

Vulnerability scanning: This involves scanning the system for known vulnerabilities that could be exploited by attackers. This can be done using automated tools or manually.

Code review: This involves reviewing the source code of an application to identify potential vulnerabilities, such as buffer overflows, injection flaws, and authentication issues.

Risk assessment: This involves identifying and evaluating the risks associated with a system. Risk assessment methodology involves the identification and mitigation of security risks associated with various assets within an application or a network.

Security auditing: This involves reviewing the security of a system to ensure that it meets security best practices and standards. You can employ a Vulnerability Assessment and Penetration Testing company to perform a security audit of your systems or you can get it done internally.

Security posture assessment: A cyber security posture assessment combines all different security testing methodologies to conduct a comprehensive assessment of a network.

Some methods are more theoretical, others are more practical. As this thesis involves experiments it is better to use practical methods. Also some of the methods, such as security auditing, is meant for usage in bigger solutions and companies and is not the best choice for home server testing. Taking in consideration all this factors combination of vulnerability scanning, risk assessment and penetration testing methods will be used in this thesis. It is also possible to use code review method,if application source code is open, but it is very difficult and time consuming process, which also does not guarantee results.

Configuration selection for software and operating system that used on server machine is important part of this thesis work as it is main scope of work and main point of interest. During experiments different values for available options in configurations of software will be used. This way it is possible to imitate different situations and analyse the impact that configurations have on security of server.

Server software choice also has certain level of importance as it has direct influence on what kind of configurations are available. Another point that gives importance to software choice is reproduction of possible system that real user could have create himself. Making sure that server that is being tested is representing a possible set-up as naturally as possible, using realistic set-up will increase value and actuality of this thesis work.

Penetration testing tools choice. Software choice comes also to decision, what kind of penetration testing software is used. It is important to use penetration testing software that receives regular updates and is actively used. This will help to achieve more accurate, precise and useful data during experiments conduction. Another possibility to increase quality of received experiment data is to use multiple pieces of software, that are deigned for specific type of testing, to prevent mistakes or possibility of missing certain vulnerabilities.

Data collection is performed during experiment phase. Each set of configurations was tested under identical initial conditions. It is important to find out which configuration or combination of configuration are effective and give result by preventing appearance of vulnerabilities or their exploitation. Another points of interest are vulnerabilities that were not effected in any way by change of configurations or initially vulnerability wasn't present and change of configurations didn't effect system in any way.

Data analysis. After data is collected it is analysed. Expected result in every experiment is decrease in vulnerabilities available for exploitation or if specific exploit is tested expected

result is inability to perform this exploit or significant limitations that will make specific exploit impractical to use.

2.2 Environment and experiments description

2.2.1 Testing environment description

Following chapters will describe experiments that will be conducted in practical part of this thesis work. Choice of certain software, that is used for penetration testing and for server machine will be explained in next chapter.

To perform experiments an environment is created to imitate real network with server running service of user's choice. For this purpose VirtualBox is used, it is installed on a host machine running Microsoft Windows10. For replication of experiments can be used any other virtualization software and OS can be used. Experiment can be performed without usage of virtualization software by setting up experiment environment with real machines.[2]

VirtualBox will allow to run multiple VMs with different OS simultaneously and gives a range of flexibility in networking options inside program itself, which can help in simulation of real life environment that can be possibly used at home. In case of this thesis work two VMs will be running in VirtualBox. First virtual machine will represent a server with UbuntuServer running on it. Second machine will be used as a host for penetration testing activity and will run Kali Linux. For both Kali Linux and UbuntuServer latest versions available are used. For UbuntuServer 22.04.2LTS and for Kali Linux release 2023.1.[3, 4]

During installation of UbuntuServer the most basic options were chosen. During installation process there is option to install some of the services that are popular and are frequently used by community. One of those options is Nextcloud software that is being tested in this work. Although this option is good to choose in case person wants to save time or performs such installation first time, in case of this particular installation this option is skipped because installing it separately makes it easier to perform further configurations and gives greater control over specific elements. To install Nextcloud there is a certain software that needs to be preinstalled for Nextcloud to function correctly. Such software is web-server and database, which should be properly preconfigured.[5]

Second virtual machine was set up with Kali Linux. Similarly to first machine most of the

options are left in default state as mostly these options do not impact main goal of this works experiments. After installation is complete a software that is used for penetration testing is installed on this virtual machine. One of this Pieces of software is Armitage, it is versatile tool used for port scanning, vulnerability detection and exploitation. To perform some of the experiments and testing, other software will installed and used, for such purposes as packet analysis, password brute force attacks and web directories enumeration.[6, 7]

After installation of software on virtual machine it is needed to perform VirtualBox network adapter configuration, so that server and penetration testing machine are visible for one another. There are multiple options that can be used as network adapter type. Using documentation for Virtual Networking the best suited type for network adapter is bridged adapter. This type of adapter will allow to achieve needed connectivity for virtual machines, both machines can see and communicate to one another and have possibility for internet connection. Additionally both VMs have connectivity to host machine, which is not important for this work.[8]

Also, it is possible to expose service on home server to public network, by means of port forwarding with router in home network or using domain name, for more accurate representation of real service, as it makes sense to make services accessible outside home network, but it can expose additional points for potential security failure. As it is not main scope of this thesis work, service provided by home server will be used only inside of private network. This part is relevant in case virtualization software such as VirualBox is used to perform experiments, if real equipment is used instead, procedure for configuring network may be different.

After adapter type choice is made, it is good practice to make sure there is connectivity between virtual machines both ways, this can be achieved by using 'ping <IP>' command in terminal and replacing <IP> with other machines IP address. IP address can be found by execution of 'ip addr' command in terminal. Connection to internet can be checked by using command 'ping 8.8.8.8', which sends ping to google public DNS. When both machines have connectivity to each other and to internet it is possible to start installation of software, configuration and penetration testing parts of experiments.

For security related configurations that will be tested during experiments official documentation provided by Nextcloud is used. There are multiple options present that aim on improvement of different security aspects described in official guide. Not every solution will be used, tested and analysed not all options provide sufficient increase in security or have little effect on malicious actor ability to exploit vulnerabilities. This configurations

target variety of vulnerabilities and are intended to prevent them or completely remediate some of the vulnerabilities. With help of security configurations provided in documentation it is possible to encrypt traffic between server and client, which in return helps with prevention of man-in-the-middle attack. Also, with given options there is possibility to prevent unauthorized access to user account, limit or completely prevent password brute-force attacks, prevent malicious actor from scanning web directories on server.[9]

2.2.2 Initial testing experiment

Initial experiment will be performed on freshly installed server to set a base line for further experiments. After installing database, web server and downloading Nextcloud user needs to check if Nextcloud is available and user can register admin account, which is a first thing that has to be done after initial set up is done.

For testing of server Armitage is installed on penetration testing machine. Armitage is then launched and after that network is scanned using nmap, which is one of the options available in Armitage. When scan is complete there should appear diagram with hosts that were found during scan and additional information about this hosts that was discovered during scan, for example open ports and OS that hosts operate on.

Next step is finding vulnerabilities, which may not give any results depending on configurations chosen. Even if there are available list of attacks it doesn't necessarily means that this vulnerabilities are possible to exploit because some of the triggers may produce false positive results and further more precise analysis of results is required.

Results of scanning for attacks and possibility to exploit them will be recorded and compared to subsequent scans. After every further experiment scan for available attacks will be performed to see any possible change. It is expected to see decrease in vulnerabilities that are spotted during scan or can be exploited. Based on the results of comparison conclusion will be made on how effective is Armitage in spotting vulnerabilities and how effective is used security measures. This results will be highly dependent on first performed scan and initial effectiveness of Armitage in verifying

2.2.3 HTTPS experiment

This experiment includes testing of HTTP and HTTPS protocol and configuration of SSL for HTTPS. Before configuring SSL for web-server it is important to test HTTP for vulnerability and confirm that it is present. To do this it is needed to perform following

steps.

After installing Wireshsark to perform packet analysis, it is needed to launch it and specify filter to display packets that are sent to server running Nextcloud. After confirming that filter works correctly, it is possible to proceed to next step in which we access web page of Nextcloud. After log in page is displayed user needs to specify credentials for one of the accounts and authenticate. Pressing "Log in" button should send packet to server and this packet should be visible in Wireshark. Due to SSl not being yet configured all credentials should be sent to server in plain text, which is a serious security risk and exposure for MITM attack.[10, 11, 12]

Man In The Middle is a serious vulnerability that can lead to a loss of access to users account or personal data. To mitigate vulnerability there is need to configure SSL for web server and redirect all requests from port 80, which used for HTTP, to port 443, which used for HTTPS. Enabling HTTPS requires acquiring SSL certificate, which can be achieved by buying one provided by CA, using services like letsencrypt, which provide SSL certificate for free, but user needs to have FQDN in this case, or generate personal SSL certificate using OpenSSL, which comes preinstalled on majority of Linux distributions for server. In case of this experiment personal SSL certificate will be generated, because FQDN is not used. Enabling HTTPS for different web-servers may differ, but generally follows same basic steps. Guide with needed configurations is used to enable HTTPS.[13]

After HTTPS is enabled experiment can be repeated. From very beginning it should be noted that traffic between client and server is encrypted and no longer vulnerable for MITM attack. Due to traffic being encrypted it is also shouldn't be possible to spot packet with username and password of user that were used to log in. If all packets are encrypted than it means that configurations is successful and and result of experiment is positive, because communication between client and host is not vulnerable to Man In the Middle Attack.

2.2.4 Data directory experiment

Next experiment will include a configuration from document by Nextcloud, which suggests to place data directory outside of Web root. Although it is recommended to do this on a new installation, procedure in this experiment will be different. This action can help in making malicious actor not being able to reach for data folder, which contains all files that user had uploaded to

There is a prior scan for vulnerabilities which is done with help of OWASP DirBuster. After collection of data regarding available vulnerabilities is done, data folder can be

moved.[14, 15]

First a backup of existing data is done in case something goes wrong or breaks. Then data directory is placed to a different location. Needed change of configurations should be done for Nextcloud, so it functions properly.

If all changes are applied successfully, which can be checked by visiting Nextcloud Web page. If web page is loaded and it is possible to log in then everything is good to go and it is possible to proceed to testing.

Second time testing will follow same procedure as a first one. After that all required data is collected and compared to a first testing results, it is possible to make a conclusion about effectiveness and usability of this security and hardening option.

2.2.5 Password brute force experiment

During next experiment capabilities of Nextcloud to prevent password brute force attacks will be tested. To evaluate this feature of Nextcloud we first need to conduct a test without this feature enabled. It is likely that this feature may be enabled by default, so first step is to check, if it is already turned on.

If this feature is already turned on, it makes sense to first test functionality and effectiveness of this security configuration and after first test is done, disable it and test Nextcloud without this feature enabled. Because testing procedure stays the same and the only thing changing is configuration, the order in which tests are performed is not important.

To test this feature a password brute force attack will be performed using Hydra. It is suggested that username is known to malicious actor and only thing that needs to be brute forced is password. For attack rockyou.txt is used and it is modified with correct password added somewhere in the middle of file. It is done due to fact that this test focuses on ability of brute force attack prevention mechanism to successfully deny possible password attacks. Theoretically IP address that is used to perform attack should be added to blacklist sooner then it reaches middle of the file.[16, 17]

As result of testing it is expected to see IP address from which attack is performed blacklisted, when feature is turned on. When this configuration is disabled it is expected that attack will be successful due to correct password being present in file that is used for attack. Also, results and conclusions of this configuration will be compared to results of next experiment, because it will cover different tool that is used for same purpose.

2.2.6 Fail2ban experiment

This experiment will test another suggestion provided in guide for Nextcloud hardening and security. This option is setup of fail2ban, which is used to prevent password brute force attack. Although, Nextcloud has built in mechanism to prevent such attacks, guidance suggests to use fail2ban instead. Fail2ban is a service that uses iptables to automatically drop connections for a pre-defined amount of time from IPs that continuously failed to authenticate to the configured services.[18]

Results of testing without any password brute force prevention mechanism can be taken form previous experiment, to compare them with results that were achieved during testing of fail2ban.

To install fail2ban on Ubuntu distribution it is simply comes to executing command 'sudo apt-get install fail2ban'. After fail2ban is installed, it is needed to create two files: one of those files defines filter that is used to spot and monitor failed login attempts, another configuration file will be used to determine, what variables are used and to which log file filter file is applied.

After both configuration files are created it is possible to perform testing procedure. For testing Hydra is used in the same way it was used in previously described experiment.

Results of this testing should be a ban of certain IP address for period of time defined in one of the configuration files. Based on the results evaluation of this security measure will be performed. Also, fail2ban will be compared to default mechanism present in Nextcloud.

3. Server software choice

3.1 Software comparison

Operating system doesn't have to be very complex for this thesis work. GUI is no required, which yields options, such as Debian, Linux Mint and Ubuntu Server. Both Linux Mint and Ubuntu are easier to deploy and configure, although Ubuntu has better compatibility with hardware and support, which makes it better candidate to use it in this work.[19, 20]

As main application there are two options for self-hosted cloud storage services: ownCloud and Nextcloud. Nextcloud seems to be a better option, since it is more flexible, has more integration options with other services, more frequent security updates and greater focus on community-driven development.[21]

To run Nextclloud it is required to install additional software, such as web server. Apache and Nginx are both great options for this purpose, but in this case Apache is more favorable, as it has greater compatibility with PHP based applications, is easier to configure and has better documentation. Also it is recommended to use Apache according to documentation of Nextcloud.[22, 23]

Last thing that needs to be installed on server machine for Nextcloud to work correctly is database. Currently Nextcloud supports following database: MySQL/MariaDB, PostgreSQL and Oracle. Out of all this options MariaDB was picked, because it is lightweight and has great performance.[24, 25, 26, 27, 28]

3.2 Ubuntu Server

Ubuntu Server is one of the popular Linux distributions for server deployments. It has certain set of traits that defined choice of it for operating system.

Easy to install and manage: Ubuntu Server has a simple and user-friendly installation process. Installation process is very straight forward and resulting installation has certain set of software pre-installed, if standard installation is picked. Some of this software will be used during tests and configurations.

Large and active community: Ubuntu Server has a large and active community of users

and developers. It is significant factor for this thesis as it will simplify search of certain solution, documentation or guides.

High level of security: This thesis work focuses on testing and security. Ubuntu Server has a strong focus on security, with regular security updates and patches available. It also includes built-in security features, that help to protect the server from potential threats.

Compatibility with various hardware and software: Ubuntu Server is compatible with a wide range of hardware and software, making it a versatile choice for server deployments. This includes support for virtualization technologies. This is especially important for this thesis work as testing environment will be created with help of VirtualBox virtualization software.

Cost-effective: Ubuntu Server is an open-source software, which means that it is free to use and distribute. This makes it a perfect choice for this work and is important.

Overall, Ubuntu Server offers a powerful, reliable, and easy-to-use server operating system that can be customized to meet the needs of deployment that will be created for testing environment during practical part of this thesis work.

3.3 Nextcloud

Nextcloud is a popular open-source file sharing and collaboration platform that provides a range of advantages, including:

Data ownership and control: Nextcloud allows users to own and control their data, as it can be self-hosted on a personal server or hosted on a private cloud. This is one of the reasons Nextcloud is picked as it can be easily self-hosted on personal server.

Security: Nextcloud is designed with security in mind, with features such as two-factor authentication, encryption, and data access control. These features help to protect sensitive data from potential security threats. Emphasis of this thesis work on security

Open-source community: Nextcloud is an open-source platform, which means that it has a large and active community. This community provides support, resources, and contributions to the platform, helping to improve its functionality and security. It greatly simplifies process of finding answers and solutions to problems or specific configurations that are needed for this thesis work.

Nextcloud provides a range of advantages that make it a powerful and versatile platform for file sharing and collaboration. Its emphasis on data ownership and control, security features, and open-source community make it a popular choice for individuals, businesses, and organizations, which also makes it a great candidate for testing due to its popularity.

3.4 Apache2 web server

Apache2 is a widely used open-source web server software that offers several advantages and disadvantages, which are as follows:

Advantages: Cross-platform support: Apache2 is compatible with most operating systems including GNU/Linux, Microsoft Windows, and Mac OS. This also means that it is suitable for environment being created in this thesis work.

Easy to configure: Apache2 has a simple configuration file structure, which makes it easy to configure and customize according to the specific needs of the website or application.

High performance: Apache2 is designed to handle a large number of concurrent connections and requests, making it a high-performance web server software.

Security: Apache2 offers several security features, such as SSL/TLS support, authentication, and access control, to help secure the web server and its applications. SSL is one of the security features that are tested in this thesis work.

Memory usage: Apache2 can be memory-intensive, especially when handling large traffic loads or when using many modules. Although, this shouldn't be an issue in this work as large traffic loads aren't expected during experiments.

Configuration complexity: Configuration file structure can be complex and overwhelming. Making configuration file correctly formatted and all need properties specified can take a lot of time. Mistakes that are made in configuration files can be checked in error logs for Apache2, which simplifies process of getting it to correct state.

Performance overhead: Apache2 may have a higher performance overhead compared to other lightweight web server software, which may be more suitable for low-traffic websites or applications.

Lack of modern features: Apache2 may not offer some of the modern features available in other web server software, such as built-in load balancing or support for HTTP/2.

Overall, Apache2 is a powerful and versatile web server software that can handle a wide range of web applications and traffic loads. However, it may not be the best choice for all use cases, and it is important to consider its advantages and disadvantages when deciding whether to use it for a specific website or application.

3.5 MariaDB

MariaDB is an open-source relational database management system (RDBMS) and a community-driven fork of the popular MySQL database. Here are some advantages of using MariaDB:

Open-source: MariaDB is a fully open-source database system that is free to use, modify, and distribute.

Performance: MariaDB has been designed for high performance and scalability, making it a good choice for large-scale applications or websites with high traffic loads.

Security: MariaDB has many security features built-in, such as encryption at rest and in transit, improved user authentication, and more.

Community-driven development: MariaDB has a large and active community of developers, which means that bugs and security vulnerabilities are often discovered and fixed quickly.

Overall, MariaDB is a robust, high-performance, and feature-rich database management system that offers several advantages over MySQL and other RDBMS solutions. Its compatibility with MySQL and open-source nature make it a popular choice for web developers and businesses of all sizes.

4. Penetration testing software choice

4.1 Software comparison

For operating system choice there are multiple variants, such as Kali Linux, Parrot Security OS and BlackArch. BlackArch is OS designed for penetration testing and has lots of different tools for this purpose, but this distribution is not very user friendly and use its potential it requires a lot of configurations. Parrot Security OS shares a lot in common with Kali Linux and also emphasises secure development. However it has problems with regularity of updates and driver, which can be an issue during usage in virtualization software. Kali Linux one of the best OS for penetration testing, that has variety of tools, definitely suitable for running as VM and is easy to install and configure, which makes it a great candidate for this thesis work.[29, 30]

To do initial testing it is required to use vulnerability scanner tool. One of the options is Nessus, but as many other vulnerability scanners it is not free. On the other hand there is option to use Metasploit as it also has option to exploit found vulnerabilities. But as Metasploit is a command line tool it may be difficult to use, as an alternative there is Armitage, which is graphical tool for Metasploit. This way it is possible to visualize data acquired during scanning and simplifies scanning and exploitation process.[31, 32]

HTTP/HTTPS testing requires analysis of packets. One of he options is to use BurpSuite, which is tool for security testing of web applications and can be used for packet analysis. Although it is versatile tool, it also has features, that can not be used in free version, which gives certain limitations and BurpSuite is not open source. On the other hand Wireshark is free, open source and is specificaly made for packets analysis. Decision to use Wireshark for this experiment was made.[33]

To perform brute-force attack experiment, it is required to obtain tool that suits for this. There are three candidates for this role: Hydra, Medusa and Burp Suite. Burp Suite is used for web application testing and has various functionality to perform testing and there is option to use this tool for password brute-force attack. One significant drawback is significant limitation in available tools and speed of operations, if free version of Burp Suite is used. UI of Burp Suite is not very user friendly and it can be resource intensive, which is a drawback in case of VM. This factors make it less favorable to use. Both Hydra and Medusa are command line tools, made specifically for brute-force attacks and are very

similar. It was decided to pick Hydra as it seems to be more popular and have greater performance.[34]

Data directory experiment requires to use tool designed to brute force directories and files names on web/application server. Just as mentioned previously Burp Suite has capabilities to perform such directory and files enumeration, but speed limitation applies to this tool as well, if free version of Burp Suite is used. On the other hand OWASP DirBuster is completely free and comes with useful wordlists, that are designed to successfully find files and directories

4.2 Kali Linux

Kali Linux is a popular GNU/Linux distribution that is specifically designed for penetration testing, ethical hacking, and digital forensics. It provides a range of advantages, including:

Powerful penetration testing tools: Kali Linux comes pre-installed with a wide range of powerful penetration testing tools that are designed to help users find and exploit vulnerabilities in networks and systems.

Large and active community: Kali Linux has a large and active community of users and developers, which provides support and resources for users. This includes online documentation, forums, and tutorials.

Compatibility with various hardware and software: Kali Linux is compatible with a wide range of hardware and software, making it a versatile choice for penetration testing and digital forensics. This includes support for various hardware architectures and virtualization technologies. Which is important, because machine with Kali Linux will be deployed with help of VirtualBox.

Regular updates and patches: Kali Linux is regularly updated with new features, tools, and security patches. This helps to ensure that users have access to the latest tools and features, and that the operating system remains secure.

Free and open-source software: Kali Linux is free and open-source software, which means that it is available for anyone to use, modify, and distribute. This makes it a free option for individuals that are looking for a powerful and versatile operating system for penetration testing and digital forensics. Which perfectly suits this thesis work.

Overall, Kali Linux provides a powerful and versatile platform for penetration testing,

ethical hacking, and digital forensics. Its powerful penetration testing tools, large and active community, high level of compatibility with various hardware and software, regular updates and patches, and free and open-source software make it a popular and effective choice for penetration testing.

4.3 Armitage

Armitage is a graphical user interface for the Metasploit Framework, which is a popular tool for penetration testing and ethical hacking.

User-friendly interface: Armitage provides a user-friendly interface that makes it easy for users to navigate and use tools of the Metasploit Framework.

Automation of common tasks: Armitage automates many of the common tasks associated with penetration testing, such as scanning for vulnerabilities, identifying targets, and launching attacks. This can help to save time and increase productivity.

Visual representation of network topology: Armitage provides a visual representation of network topology, which can help users to identify potential attack vectors and vulnerabilities in target systems. It is less of a concern in this work as topology of network during experiments is very simple.

Integration with other tools: Armitage can be integrated with a range of other tools and platforms, such as Nessus and Nmap, which can help to enhance its functionality and provide additional capabilities.

Open-source software: Armitage is open-source software, which means that it is available for anyone to use, modify, and distribute. This makes it free, powerful and versatile tool for penetration testing and ethical hacking.

Overall, Armitage provides a powerful and user-friendly interface for the Metasploit Framework, which can help users to identify vulnerabilities in their target systems and launch effective attacks. Its automation of common tasks, visual representation of network topology, integration with other tools, and open-source software make it a perfect choice for this thesis work.

4.4 Wireshark

Wireshark is a popular open-source network protocol analyzer that is used for troubleshooting, analysis, and security testing. Here are some of its advantages and disadvantages:

Rich feature set: Wireshark has a rich feature set that allows for deep analysis of network traffic. It can capture and decode hundreds of different network protocols, and provides filtering and search capabilities.

Cross-platform support: Wireshark is available for multiple operating systems, including Microsoft Windows, Mac OS, and GNU/Linux, which makes it a versatile choice for network analysis and also suitable in case of this thesis.

Community support: Wireshark has a large and active community of users and developers, which provides a significant amount of support and resources. This includes online documentation, forums, and tutorials.

Open-source software: Wireshark is free and open-source software, which means that it is available for anyone to use, modify, and distribute. This makes it a free option for individuals that are looking for a powerful and versatile network analysis tool. Which perfectly suits for this thesis work.

Steep learning curve: Wireshark has a steep learning curve. Some of its features are not that easy to use and most of the time UI is not very user friendly and is hard to perceive.

Resource-intensive: Wireshark can be resource-intensive, particularly when analyzing large volumes of network traffic. This can cause slow performance on less powerful hardware or virtual machine. This may be a concern during this work, because penetration testing machine is also used with help of virtualization software. Although it is expected that amount of traffic will be mild in testing environment.

Legal considerations: Wireshark can potentially be used for malicious purposes, which means that users need to be aware of legal considerations. As this tool is used in experiment environment that is set in private network it shouldn't be an issue.

Overall, Wireshark provides a powerful and versatile tool for network troubleshooting and analysis of packet.

4.5 Hydra

Hydra is command-line tool used to perform brute-force attacks on servers and applications. It has certain advantage and disadvantages.

Customizable: Hydra provides user with different parameters that can be specified to achieve desired result. It is possible to choose type of attack and wordlist that will be used to guess password or username.

Fast and lightweight: Hydra can test a large amount of possible combinations for username and password in short period of time.

Legality: Usage of this tool may be illegal and can get a person in trouble. During this work it shouldn't be a problem, because all experiments are performed in test environment.

Difficulty of usage: Flexibility and customizability of Hydra also brings sometimes unnecessary difficulty to user experience.

4.6 OWASP DirBuster

DirBuster is a tool used for directory and file enumeration on web servers. It has certain advantage and disadvantages.

Customizable: DirBuster is highly customizable, allowing to configure various parameters such as the type of attack, the wordlist to use for directory and file enumeration, and the extensions to search for.

Supports multiple protocols: DirBuster supports multiple protocols, including HTTP, HTTPS, and FTP. In case of this thesis work HTTPS protocol will be used.

Open-source: DirBuster is open-source, which means that it is free to use, and the source code can be audited for security vulnerabilities.

Easy to use: DirBuster has a user-friendly interface, making it easy to use .

Can be time-consuming: Scanning with DirBuster can take a lot of time.

False positives: DirBuster can generate a large number of false positives, which can be

time-consuming to manually review.

Can cause server overload: DirBuster can cause server overload by sending too many requests.

5. Practical part

This chapter of thesis is intended to describe initial set up of experiment environment that was done by author to do experiments and detailed process of performing this experiments. Every experiment includes description of actions that were taken to perform experiment, what actions were taken to achieve proper results and short conclusion with achieved results.

5.1 Initial set up and configurations

To do any of the following experiments it is needed to perform initial set up of server machine that will be tested. Software that will be tested is Nextcloud. To start Nextcloud on server there are certain requirements, because it is not a stand alone software and requires additional programs to run it.[35]

First program that is needed for installation of Nextcloud is web server that will serve our application. As web server Apache2 was chosen because of certain factors that are mentioned in previous chapters and also because it is recommended by Nextcloud developers. To install Apache2 command sudo apt install apache2 is executed in terminal. Successful installation can be verified by visiting default page in web browser, which can be achieved by specifying server machine's ip address as URL that we want to visit. If it is not possible to visit default page it is likely that port 80 is not open on server. This port can be opened with help of UFW by execution of 'sudo ufw allow 80' command. After installation of web server next step is to create configuration file that will allow to serve application instead of default html page.

Second piece of software that is needed to run Nextcloud is database. For database MariaDB was chosen for the reasons previously described. MariaDB is installed on server by execution of 'sudo apt install mariadb' command. After installation is complete next step is creation of database that will be used by Nextcloud to store needed data of users and their credentials. It is important to remember credentials and database name as it is required in further steps for installation.

Last step is download of Nextcloud itself it is done by downloading tar archive from official nextcloud site. After tar archive with application is downloaded next step is unzip it to directory of choice, in this case default directory /var/www/html is used. Because web

server was installed and configured in previous step Nextcloud should be now available.

First thing that has to be done after visiting Nextcloud first time is creation of administrative account and specifying information about database to connect Nextcloud to it. This is why it is important to remember information that was specified in during creation of database in MariaDB.

5.2 Initial testing experiment

This experiment is performed to get baseline for further tests that will be conducted and evaluate overall security level of initial setup for server that runs Nextcloud. To perform this test on machine that runs kali linux for penetration testing a software called armitage is installed by execution of command 'sudo apt install armitage'.

After armitage is installed it can be launched by running command 'sudo armitage' in command line. Following instructions that appear on the screen Armitage should be now launched and ready for work.

First step in armitage is to perform scan, which is done by navigating to left-upper corner and clicking 'Hosts' button, which drops menu with options. We can manually add host by picking option 'Add Hosts...' and specifying IP address of host we want to add. In case of this exact experiment option 'Nmap Scan' is picked and option 'Quick Scan (OS detect)'. After that window appears with request to specify address range, in this field needed range '192.168.0.0/24' is given to find needed host. After that table should be populated with hosts that were found.

Host that interests us has IP address 192.168.0.104 and icon of this host indicates that it is running GNU/Linux distribution, which can be also seen by hovering mouse cursor over icon and displaying that in this case it is 'linux 5.x'

After initial scan is performed it is possible to scan host for attacks. This can be done by navigating to 'Attacks' menu and selecting 'Find Attacks' option. This scanning procedure takes some time and after it is complete a new option called 'Attack' appeared in host menu, which called by Right clicking host icon.

Although 'Attack' menu is populated we different kinds of vulnerabilities it doesn't mean that target host has services that are potential source of this weaknesses. To simplify process a flood attack is initiated by choosing 'Hail Mary' option in 'Attack' menu. This will automatically launch all possible attacks for hosts.

Unfortunately all this steps didn't yield any results on target host, even though in available attacks there are options for services that are running on server machine, such as apache2 web server. It is still doesn't mean that target host is completely secure and not susceptible to other types of attacks and vulnerabilities.

5.3 HTTPS experiment

During this experiment SSL certificate and HTTPS will be configured and tested. Test will be performed with help of Wireshark.

Initially apache2 web server was not configured to serve Nextcloud via HTTPS protocol and it runs on http which makes communication between client and server being sent in plain text. To check this, wireshark is started to intercept packets. First interface that will be used by Wireshark to sniff packets is chosen, in this case it is eth/0 because it is interface that is used by penetration testing machine to connect to network. Traffic of communication of other machines on network should be seen.

It is needed to apply filter to display only traffic that is important for this experiment. To do this we to filter field line 'dst.ip=192.168.0.104' to display only traffic that is sent to server machine. After that web page of Nextcloud is open in browser and login to one of the user accounts is performed. This sends request web server and produces traffic that now can be examined. One of the packets that was sent is POST request, which was generated after 'Log in' button was clicked. Clicking on this packet and expanding its properties displayed credentials that were used to log in. Enabling HTTPS should make all traffic encrypted

To enable HTTPS first step is to generate self-signed, this is done using openssl, which comes preinstalled on UbuntuServer. Key and certificate are generated. After that configuration file that is used by apache2 to run nextcloud is modified: all traffic that is received on port 80 is redirected to port 443, HTTPS is enabled and path to SSL certificate and key is specified. To apply changes apache2 web server is restarted to apply changes by executing command 'sudo systemctl restart apache2.service'.

Next step is testing of HTTPS. Just like in step of testing before enabling HTTPS Wireshark is used and configured to display traffic that is sent to web server. Accessing Nextcloud web page and performing login same as before generates traffic, but closer examination shows that all data that is exchanged is now encrypted, which doesn't prevent unwanted interception of client to server communication, but allows for secure data exchange over public channel and prevents MITM attack.

5.4 Data directory experiment

This experiment will test, what kind of impact on security can be if data directory for Nextcloud is located outside of Nextcloud root directory. This option is suggested by Nextcloud team in guide on hardening and security.

DirBuster is installed on penetration testing machine by execution of command 'sudo apt install dirbbuster'. After it is launched, to start testing URL needs to be specified 'https://192.168.0.104/' and wordlist that will be used to perform scan '/usr/share/wordlists/dirbuster/directories.jbrofuzz'. Also 'be recursive' option is disabled and option 'Use Blank Extension' is enabled. After scan is completed 21 directory or file was shown, most of them don't poses any security risk. Result also displayed data directory, but there is nothing displayed in this folder if user tries to view it in web browser. Other interesting file is 'status.php', which shows information about application including version of Nextcloud.

To move directory it is needed to first create backup copy of it in existing directory of Nextcloud, which is done by navigating to Nextcloud root directory '/var/www/html/nextcloud' and executing 'sudo cp -r data data.backup'. This way in case something goes side ways, it is possible to restore a previous state of data folder and start experiment from beginning.

Next step is moving data folder to a new location, for this purpose a directory '/var/opt/' was picked. Data directory is moved by executing command 'sudo mv /var/www/html/nextcloud/data /var/opt/nextcloud/data'. Also it is required to change configuration file of Nextcloud and specify new location of data directory by adding or replacing existing line.

Next step is to check if changes were applied successfully, this is done by navigating to web page and authenticating with one of the user accounts. Next new text document is created in documents app for this user. If all changes were successful and configuration file is correct, document that was just created is now visible in user specific data directory.

Next step is to launch DirBuster with same configurations as in previous testing, before data directory was moved.

As result data directory didn't appear in tree view of finished scan, which is a result of moving this directory to different location. This effectively doesn't expose this directory to internet, which potentially could lead to lose of sensitive and personal information.

5.5 Password brute force experiment

This experiment will test built in functionality of Nextcloud to prevent brute force attacks. By default this functionality is enabled and it is highly encouraged to not turn it off. To perform test during conduction of this experiment a hydra software is used.[36]

Hydra is installed on penetration testing machine by executing 'sudo apt install hydra' in command line. Hydra is command line tool. To run it we first need to get certain information from login page. One of those is URL of login page, header that is sent with POST request, when 'login' button is pressed and something that will indicate unsuccessful attempts, in this case 'Wrong username or password.'. Second element that is needed for command is header that is sent, when login button is clicked, which can be found with help of developer tools in web browser. Knowing all this information it can be added to hydra command, where /usr/share/wordlists/rockyou.txt is a wordlist that contains correct password. It is suggested that username is already known to malicious actor.

Executing this command didn't yield any successful matches. Accessing Nextcloud login page from same machine that was used to perform attack will display message 'We have detected multiple invalid login attempts from your IP. Therefore your next login is throttled up to 30 seconds'. It is a clear sign that there is certain functionality that prevents brute force attacks and it is enabled.

This brute force prevention mechanisms can be disabled by adding certain lines to configuration file of Nextcloud: "'auth.bruteforce.protection.enabled' => false," and "'ratelimit.protection.enabled' => false,". After new configurations added and changes of file are saved, server machine was restarted to make sure new configurations are applied.[37]

Same command is executed to perform brute force attack with hydra. Due to penetration testing machine running with help of virtualization software, this command took some time to output result, that showed correct combination of username and password for user account. Accessing login page from penetration testing machine this time didn't show any timeout message for login attempts.

Although default mechanism prevents malicious actor from making a lot of login attempts by adding 30 seconds timeout between login attempts, it is still possible to perform brute force attack, but it will take a lot more time then without this mechanisms in place. This is why it is not recommended to disable this features.

However it is possible to turn off brute force prevention mechanisms, in case there are

other security measures in place, such as 2FA, password policy that is stronger then default one, other prevention mechanisms or software such as fail2ban.

5.6 Fail2ban experiment

Fail2ban is alternative that can be used with or instead of default options that are used to prevent brute force attacks. It is installed separately on server machine and configured to filter for certain entries in log file and can be installed and configured to moderate traffic for variety of services.

To install fail2ban 'sudo apt install fail2ban' command is executed to install. Now it is needed to create configuration files that are required for fail2ban to perform moderation for Nextcloud. Two files are required - first file is created in /etc/fail2ban/filter.d/ and called nextcloud.conf. A filter defines regex rules to identify when users fail to authenticate on Nextcloud's user interface, WebDAV, or use an untrusted domain to access the server. Second file is created in directory /etc/fail2ban/jail.d and named nextcloud.local. The jail file defines how to handle the failed authentication attempts found by the Nextcloud filter.

After new files are created it is required to restart fail2ban process by execution of 'sudo systemctl restart fail2ban.service'. It is possible to check status of configurations for nextcloud by execution of 'fail2ban-client status nextcloud' command, which also displays banned IP addresses.

To test this feature Hydra is used with same command that was used in Password brute force experiment and same wordlist with added correct password is used in this command. After 3 consecutive failed login attempts IP address of penetration testing machine is added to ban list for 86400 seconds or 24 hours.

Fail2ban proofs to be more flexible and customizable then default functionality provided by Nextcloud. In combination with other functionality like 2FA, strong password policy and default mechanisms built in Nextcloud, it is possible to minimize possibility of someone, who performs brute force attack, achieving success.

6. Analysis of experiments results

Conducting experiments during this thesis work yielded results, that can be analysed and based on this results conclusion about effectiveness of security related measures and configurations can be made. Also during analysis process performance of penetration testing software is evaluated, as it also played certain part in final results.

First experiment didn't give expected results. Performing vulnerability scan with Armitage gave a list of possible vulnerabilities that can be present on server machine, but majority of this vulnerabilities are for software that is not present on server machine. After completing exploits that were available for execution, not a single one was executed successfully. One of the reasons, why it happened, can be due to Metasploit database not having relevant exploits for Nextcloud and other components that are used on server machine.

Even with Armitage not being able to spot any problems in experiment environment, it is still can perform better and help with fast and simple scanning of hosts in other situations and more complex scenarios with greater amount of hosts and software that can be run on this hosts.

Data directory experiment also didn't give expected results. During testing procedure with OWASP DirBuster no vulnerabilities were found before as well as after moving data directory outside of Nextcloud root directory. After first scan data directory was visible, but accessing it didn't display any sensetive information Even without real exploit that can be used in this situation, moving data directory to a different location can prevent vulnerabilities, that are yet to be discovered and also has benefit of keeping application code and data in different locations, which can prevent such problems as data loss during update of application if it is performed manually, which to some extent can also be considered a security measure as it helps to prevent data loss. Also, after moving directory form Nextcloud root directory, it wasn't visible during second scanning.

Three experiments out of five were successful and expected results were achieved.

Results that were achieved during HTTPS experiment are as expected. After creating SSL certificate and configuring Apache2 web server to serve Nextcloud over HTTPS, all traffic that was previously exchanged between client and server in plain text was now encrypted, which greatly increased security of application and helped to mitigate man-in-the-middle

attack.

Password brute-force attack experiment showed, that default mechanisms made to prevent such attacks can increase security of system by limiting amount of login attempts that can be made from specific IP address. Although this kind of prevention method is effective it doesn't completely prevents password brute-force attacks.

In fail2ban experiment it was found out, that this tool can be a lot more effective then default brute-force attack prevention mechanisms. It proves to be not so easy to configure for every specific application and can take a lot of time, if there is no proper guide available. After fail2ban filter is correctly configured it proves to be very customizable and it is easy to fine tune it for specific scenario to minimize false positive blocks and maximize effectiveness of brute-force attack prevention.

If fail2ban and default prevention mechanisms are used at the same time, stronger password policy is applied and 2FA is forced to be used by every user, this way it will make brute-force attack almost impossible to execute. In this case only feasible option to get access to user account is social engineering, which is out of this thesis scope.

Table 1. *Experiments results*

Experiment	**Before applying configuration**	**After applying configuration**
HTTPS experiment	Data exchanged between server and client in plain text. It is possible to intercept data and credentials.	Encryption of data exchange between client and server. Communication is secure and it is impossible to intercept data.
Data directory experiment	Data directory is visible after scanning server. It is impossible to access contents of data directory. Also other files and directories discovered.	Data directory is not visible after scanning performed. Other files and directories persisted.
Password brute force experiment	Using Hydra and wordlist it is possible to perform successful password brute force attack.	It is harder to perform brute force attack due to 30 seconds timeout, that appears after certain amount of unsuccessful login attempts, but still possible.

Continues...

Table 1 – *Continues...*

Experiment	**Before applying configuration**	**After applying configuration**
Fail2ban experiment	sing Hydra and wordlist it is possible to perform successful password brute force attack.	After certain amount of unsuccessful login attempts IP, that is used for login, is banned for predefined period of time.

7. Future research

This work has huge potential in future researches. There is many other aspects, variables and conditions that can result in different outcomes of experiments and testing procedures.

First variable that can be changed is version of Nextcloud itself. Testing of older versions is relevant, because Nextcloud has app store with different add-on options. Situation, when new version of Nextcloud is released and some add-on is not yet compatible with it, may stop administrator from updating to latest version, because users heavily rely on this add-on, which can result in server being exposed to vulnerability that is still available for exploitation on older version.

Newer version that are yet to be released are also subjects to testing, as new features that are added or changes in application source code, may result in appearance of new vulnerabilities.

Add-on from Nextcloud app-store are also may add security risk to system, as they extend functionality of Nextcloud, which can result in exposure of vulnerabilities.

Change of key elements in experiment environment, such as OS, web-server or database, also can result in different results of experiments, because other software that can be used instead one that was used in this work, may lack features, that are present in software that was tested during this work. As well other elements can add new security related features. Software that is used for testing, also can be changed or its analogues can be used.

Also, it is important to notice that even in environment that was created for testing in this particular thesis work, not all security features, mechanisms and configurations were tested. Based on this different options, that weren't tested, it is possible to come up with new experiments in future research, that will test them.

8. Summary

Configurations and security solutions were applied to create testing environment and after that using tools, that are best suited for each individual solution, this configurations were tested. After that acquired information was compared to testing results of application before security related changes were applied to server.

As result evaluation of effectiveness of each component was done. Advantages, disadvantages and problems, that can possibly appear during implementation of this solutions, were brought. Also, recommendations about usage and implementation of each option, that was tested, were given.

This way goals of this thesis work were achieved by successfully implementing and testing security related solutions, that were picked by author, following official security and hardening guide for software that is used in testing environment. Out of five experiments only one yielded unexpected results, but as this experiment was intended to test security of initial system overall and didn't target specific configuration, it is considered as success, because initial condition of system was secure enough for Armitage to not find any exploitable vulnerability.

References

[1] Saumick Basu. *6 Security Testing Methodologies Explained: Definitions, Processes, Checklist*. [Updated: 23-08-2022]. URL: https://www.getastra.com/blog/security-audit/security-testing-methodologies-explained.

[2] *VirutalBox official page*. [Accessed: 15-05-2023]. URL: https://www.virtualbox.org/.

[3] *UbuntuServer download page*. [Accessed: 15-05-2023]. URL: https://ubuntu.com/download/server.

[4] *Kali Linux download page*. [Accessed: 15-05-2023]. URL: https://www.kali.org/get-kali/#kali-virtual-machines.

[5] *Nextcloud official page*. [Accessed: 15-05-2023]. URL: https://nextcloud.com/.

[6] *Armitage github repository*. [Accessed: 15-05-2023]. URL: https://github.com/r00t0v3rr1d3/armitage.

[7] *Armitage tool page*. [Accessed: 15-05-2023]. URL: https://www.kali.org/tools/armitage/.

[8] *VirtualBox Networking*. [Accessed: 15-05-2023]. URL: https://www.virtualbox.org/manual/ch06.html.

[9] *Hardening and security guidance*. [Accessed: 15-05-2023]. URL: https://docs.nextcloud.com/server/latest/admin_manual/installation/harden_server.html.

[10] *Wireshark official page*. [Accessed: 15-05-2023]. URL: https://www.wireshark.org/.

[11] *Wireshark tool page*. [Accessed: 15-05-2023]. URL: https://www.kali.org/tools/wireshark/.

[12] *What is SSL?* [Accessed: 15-05-2023]. URL: https://www.cloudflare.com/learning/ssl/what-is-ssl/.

[13] *Let's encrypt official page*. [Accessed: 15-05-2023]. URL: https://letsencrypt.org/.

[14] *OWASP official page*. [Accessed: 15-05-2023]. URL: https://owasp.org/projects/.

[15] *DirBuster tool page*. [Accessed: 15-05-2023]. URL: https://www.kali.org/tools/dirbuster/.

[16] *Hydra github repoitory*. [Accessed: 15-05-2023]. URL: https://github.com/vanhauser-thc/thc-hydra.

[17] *Hydra tool page*. [Accessed: 15-05-2023]. URL: https://www.kali.org/tools/hydra/.

[18] *Fail2ban*. [Accessed: 15-05-2023]. URL: https://www.fail2ban.org/wiki/index.php/Main_Page.

[19] *Linux Mint official page*. [Accessed: 15-05-2023]. URL: https://linuxmint.com/.

[20] *Debian official page*. [Accessed: 15-05-2023]. URL: https://www.debian.org/.

[21] *OwnCloud official page*. [Accessed: 15-05-2023]. URL: https://owncloud.com/.

[22] *Apache web server official page*. [Accessed: 15-05-2023]. URL: https://httpd.apache.org/.

[23] *Nginx official page*. [Accessed: 15-05-2023]. URL: https://nginx.org/.

[24] *Nextcloud database configuration documentation*. [Accessed: 15-05-2023]. URL: https://docs.nextcloud.com/server/latest/admin_manual/configuration_database/linux_database_configuration.html.

[25] *MySQL official page*. [Accessed: 15-05-2023]. URL: https://www.mysql.com/.

[26] *PostgreSQL official page*. [Accessed: 15-05-2023]. URL: https://www.postgresql.org/.

[27] *Oracle download page*. [Accessed: 15-05-2023]. URL: https://www.oracle.com/database/technologies/oracle-database-software-downloads.html.

[28] *Mariadb official page*. [Accessed: 15-05-2023]. URL: https://mariadb.org/.

[29] *Parrot Security OS official page*. [Accessed: 15-05-2023]. URL: https://www.parrotsec.org/.

[30] *BlackArch official page*. [Accessed: 15-05-2023]. URL: https://www.blackarch.org/.

[31] *Nessus official page*. [Accessed: 15-05-2023]. URL: https://www.tenable.com/products/nessus.

[32] *Metasploit official page*. [Accessed: 15-05-2023]. URL: https://www.metasploit.com/.

[33] *Burpsuite official page*. [Accessed: 15-05-2023]. URL: https://portswigger.net/burp.

[34] *Medusa official page*. [Accessed: 15-05-2023]. URL: http://foofus.net/?page_id=51.

[35] *Example installation on Ubuntu 22.04 LTS*. [Accessed: 15-05-2023]. URL: https://docs.nextcloud.com/server/latest/admin_manual/installation/example_ubuntu.html.

[36] *Nextcloud brute force protection*. [Accessed: 15-05-2023]. URL: https://docs.nextcloud.com/server/latest/admin_manual/configuration_server/bruteforce_configuration.html.

[37] *Nextcloud configuration parameters*. [Accessed: 15-05-2023]. URL: https://docs.nextcloud.com/server/24/admin_manual/configuration_server/config_sample_php_parameters.html.

Appendix 1 – Non-Exclusive License for Reproduction and Publication of a Graduation Thesis[1]

I Andrei Aleksejev

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Security Evaluation and Testing of Software for Home Server", supervised by Edmund Laugasson
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

15.05.2023

[1]The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.