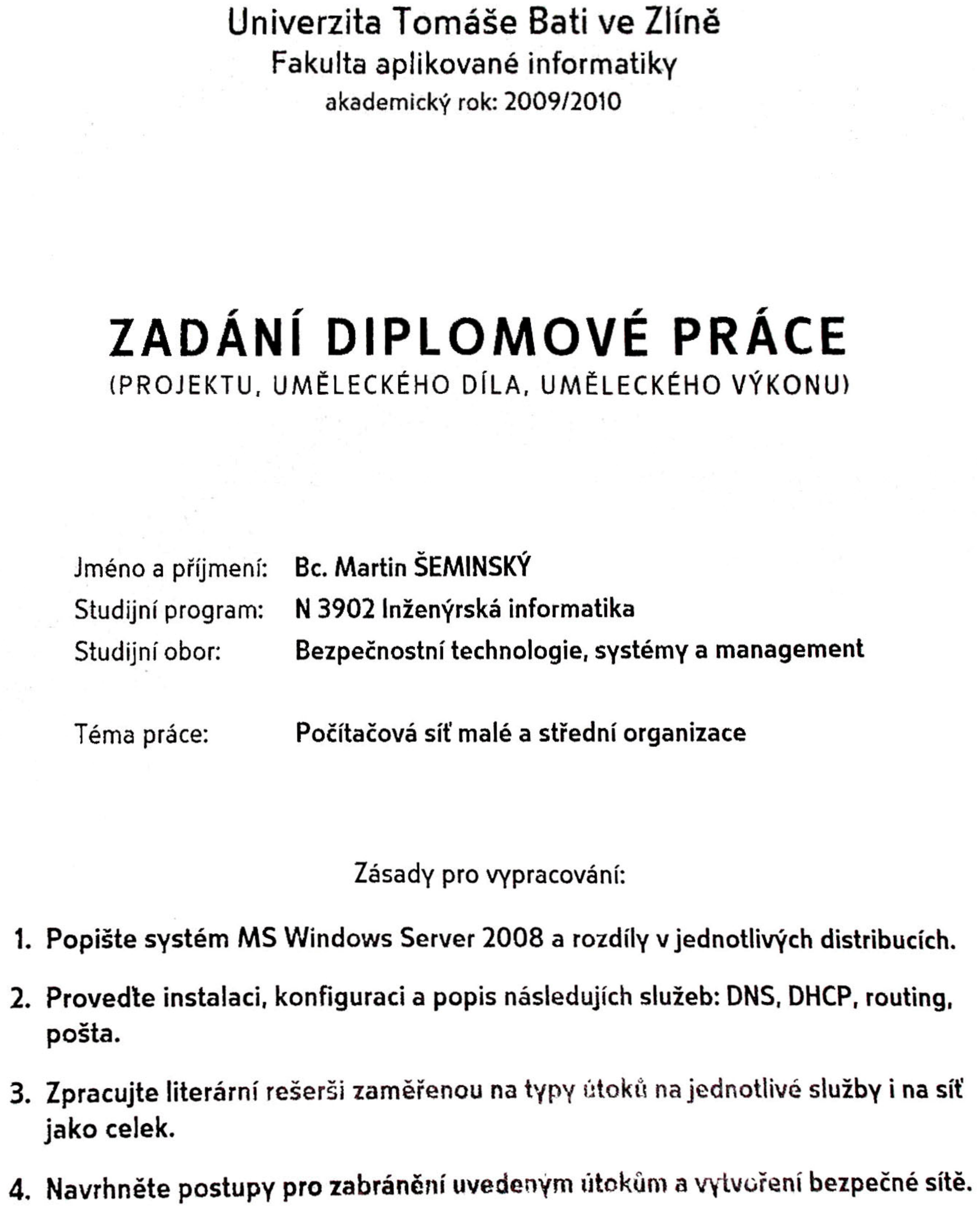
Computer Networking for Small and Medium-Sized Enterprises

Počítačová síť malé a střední organizace

Bc. Martin Šeminský

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

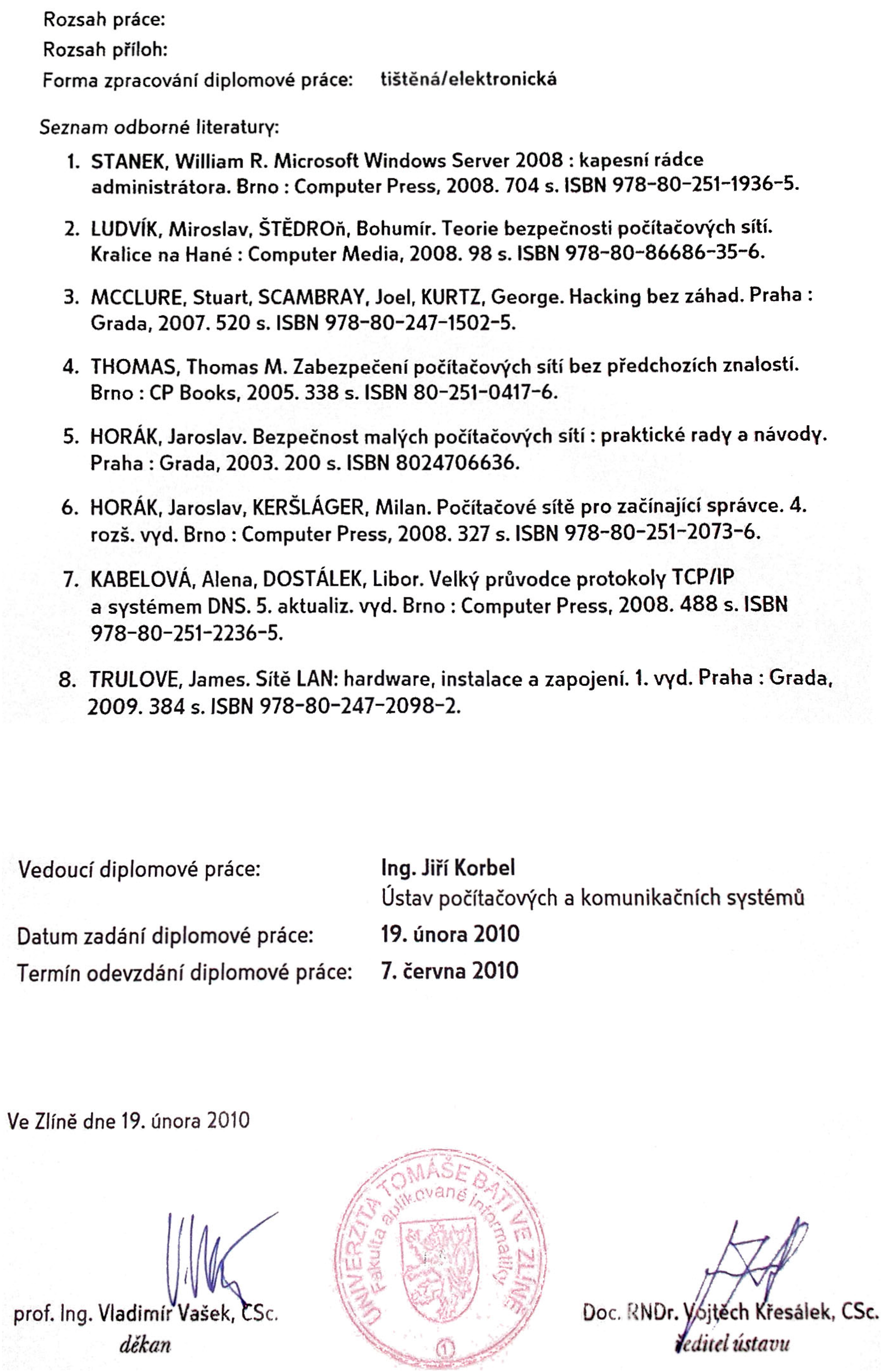
ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martin ŠEMINSKÝ**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Počítačová síť malé a střední organizace**

Zásady pro vypracování:

1. **Popište systém MS Windows Server 2008 a rozdíly v jednotlivých distribucích.**
2. **Proveďte instalaci, konfiguraci a popis následujích služeb: DNS, DHCP, routing, pošta.**
3. **Zpracujte literární rešerši zaměřenou na typy útoků na jednotlivé služby i na síť jako celek.**
4. **Navrhněte postupy pro zabránění uvedeným útokům a vytvoření bezpečné sítě.**



Rozsah práce:
Rozsah příloh:
Forma zpracování diplomové práce: tištěná/elektronická

Seznam odborné literatury:

1. STANEK, William R. Microsoft Windows Server 2008 : kapesní rádce administrátora. Brno : Computer Press, 2008. 704 s. ISBN 978-80-251-1936-5.
2. LUDVÍK, Miroslav, ŠTĚDROň, Bohumír. Teorie bezpečnosti počítačových sítí. Kralice na Hané : Computer Media, 2008. 98 s. ISBN 978-80-86686-35-6.
3. MCCLURE, Stuart, SCAMBRAY, Joel, KURTZ, George. Hacking bez záhad. Praha : Grada, 2007. 520 s. ISBN 978-80-247-1502-5.
4. THOMAS, Thomas M. Zabezpečení počítačových sítí bez předchozích znalostí. Brno : CP Books, 2005. 338 s. ISBN 80-251-0417-6.
5. HORÁK, Jaroslav. Bezpečnost malých počítačových sítí : praktické rady a návody. Praha : Grada, 2003. 200 s. ISBN 8024706636.
6. HORÁK, Jaroslav, KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. 4. rozš. vyd. Brno : Computer Press, 2008. 327 s. ISBN 978-80-251-2073-6.
7. KABELOVÁ, Alena, DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP a systémem DNS. 5. aktualiz. vyd. Brno : Computer Press, 2008. 488 s. ISBN 978-80-251-2236-5.
8. TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha : Grada, 2009. 384 s. ISBN 978-80-247-2098-2.

Vedoucí diplomové práce: **Ing. Jiří Korbel**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
1

prof. Ing. Vladimír Vašek, CSc.
děkan

Doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRACT

This thesis deals with the practical technical issues related to a computer network. In particular, the design and creation of the main functions that any networks of small or medium-sized enterprises may require. Security is discussed as main topic throughout the entire paper. It includes step-by-step configuration instructions as well as common threats to avoid.

KEYWORDS

Network, service, security, policy, password, management, Windows Server 2008, configuration, step-by-step, DNS, NAT, DHCP, POP3, SMTP, Firewall, SSL, TLS, HTTPS, IIS, WFAS.

ACKNOWLEDGEMENT

In this part, I would like to express my gratitude to all who supported my efforts during the work on this thesis. Thanks go to my supervisor, Ing. Jiří Korbel for his valuable and inspiring suggestions. The Special thanks belong to Richard Brunet-Thornton, Ph.D., whose help and advice has been crucial during the correction. Last, but not least I would like to give the thanks to my sweet mother for her devoted support during my studies with apologize to whom I have omitted.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ……………………….

podpis diplomanta

TABLE OF CONTENTS

INTRODUCTION 9
I THEORETICAL SECTION 10
1 MICROSOFT SERVER 2008 SYSTEM DESCRIPTION 11
2 DISTRIBUTIONS OF MS WINDOWS SERVER 2008 12
2.1 INTRODUCTION 12
3 REASONS FOR NETWORK SECURITY 13
4 COMPANY SECURITY POLICY 14
4.1 SAMPLE SECURITY POLICY 14
5 COMPUTER NETWORK 17
5.1 INTRODUCTION 17
5.2 ISO OSI MODEL 17
6 NETWORK SECURITY 20
6.1 OVERVIEW 20
6.2 SECURING SMALL BUSINESS 20
6.3 SECURING MEDIUM ENTERPRISES 21
7 NETWORK SECURITY - PARTICULAR PARTS OF NETWORK 22
7.1 CABLING 22
7.2 TRANSPORT LAYER - NETWORK TRAFFIC AS LISTENABLE DATA 22
7.3 SWITCHES AND HUBS 26
7.4 ROUTERS 28
7.5 HOSTS 30
7.6 COMPUTER VULNERABILITIES 30
7.7 PEOPLE 32
8 COMMON TYPES OF NETWORK ATTACKS 34
8.1 EAVESDROPPING 34
8.2 DATA MODIFICATION 34
8.3 IDENTITY SPOOFING (IP ADDRESS SPOOFING) 34
8.4 PASSWORD-BASED ATTACKS 35
8.5 DENIAL-OF-SERVICE ATTACK 35
8.6 MAN-IN-THE-MIDDLE ATTACK 35
8.7 COMPROMISED-KEY ATTACK 36
8.8 SNIFFER ATTACK 36
8.9 APPLICATION-LAYER ATTACK 36

II PRACTICAL SECTION ... 38
9 MICROSOFT SERVER 2008 INSTALLATION ... 39
10 SYSTEM CONFIGURATION ... 40
11 THE PHYSICAL NETWORK ... 42
11.1 EQUIPMENT ... 42
11.2 ROUTER ... 43
11.3 SERVER ... 43
11.4 SWITCH ... 43
11.5 CONNECTION TO THE INTERNET ... 44
11.6 PATCH CABLE ... 44
11.7 NETWORK SCHEMA ... 46
11.8 IP DESIGN OF THE NETWORK ... 47
12 USED SERVICES ... 49
12.1 ROUTING ... 49
12.2 NETWORK ADDRESS TRANSLATION - NAT ... 51
12.3 DOMAIN NAME SERVICE - DNS ... 53
12.4 DYNAMIC HOST CONFIGURATION PROTOCOL - DHCP ... 58
12.5 FIREWALL - WFAS ... 60
12.6 WEB SERVER - IIS ... 63
12.7 SECURE SOCKET LAYER - SSL ... 67
12.8 MAIL SERVICES – SMTP/POP3 ... 69
DISCUSSION ... 73
CONCLUSION ... 74
LIST OF LITERATURE ... 75
LIST OF SYMBOLS, ACRONYMS AND ABBREVIATIONS ... 77
LIST OF FIGURES ... 79
LIST OF TABLES ... 80

INTRODUCTION

Today most people understand the importance of the IT sector. The width and spread within the infrastructure pose many possible threats. These threats may cause a failure in any particular part of the IT configuration. Unfortunately, most of the threats originate from the network. This is the reason why I decided to study the principles by which to avoid them. During this research, I have found the literature at times to be too wordy and some of the “pocket handbooks” weighed more than a kilo. Therefore, I have decided to optimise the information available to new administrators and designers in their task of establishing a new computer network. In comparing the possibilities of server operational systems the Windows Server system is the superior product due to its simplicity of the administration interface as well as the low level of time spent at routine work. It supports automatic updates and some new features from past releases. The past releases often placed the system at a higher security risk or difficulty to administer was rebuilt with good results.

The concept of the thesis is made in the structural way with example network cases. The following recommended techniques lead to a stable and secured network configuration. The entire list of techniques is not mandatory as the variety of network configuration and required services running is endless.

The thesis is written for those who understand main IT principles. It contains many acronyms associated with theory. Some of these are mentioned and illustrated through underlined comment; others are commented in the list of abbreviations. In general, I found it not necessary to discuss the implications from Boolean algebra to particular algorithms applied to routing and automatic network exploration. However, some are discussed. If required, the *Internetworking Technology Handbook* published by Cisco Technologies [15] may be consulted as a reference manual.

I. THEORETICAL SECTION

1 MICROSOFT SERVER 2008 SYSTEM DESCRIPTION

Windows Server 2008 R2 builds on the award-winning foundation of Windows Server 2008, expanding existing technology and adding new features to enable IT professionals to increase the reliability and flexibility of their server infrastructures. New virtualization tools, Web resources, management enhancements, and exciting Windows 7 integration help save time, reduce costs, and provide a platform for a dynamic and efficiently managed data centre. Powerful tools such as Internet Information Services (IIS) version 7.5, updated Server Manager and Hyper-V platforms and Windows Power Shell version 2.0 combine to give customers greater control, increased efficiency and the ability to react to front-line business needs faster than ever before.[24]

Windows Server 2008 is built from the same code base as Windows Vista; therefore, it shares much of the same architecture and functionality. Since the code base is common, it automatically comes with most of the technical, security, management and administrative new features to Windows Vista. These include the rewritten networking stack (native IPv6, native wireless, and speed and security improvements); improved image-based installation, deployment and recovery; improved diagnostics, monitoring. It also encompasses event logging and reporting tools; new security features such as, Bit Locker and ASLR; improved Windows Firewall with secure default configuration; .NET Framework 3.0 technologies, specifically Windows Communication Foundation, Microsoft Message Queuing and Windows Workflow Foundation; and the core kernel, memory and file system improvements. Processors and memory devices are modelled as Plug and Play devices, to allow hot plugging of these devices. This allows the system resources to be partitioned dynamically using Dynamic Hardware Partitioning; each partition has its own memory, processor and I/O host bridge devices independent of other partition.[25]

2 DISTRIBUTIONS OF MS WINDOWS SERVER 2008

2.1 Introduction

The Microsoft Windows Server 2008 is a product application, which may exist in many various modifications. Main two types of instances are physical and virtual. The physical is installation at one server using its own CPUs directly. Virtual instance is through a virtual machine installed on physical instance of other operational system (may be the same).

For any kind of instance such as virtual or physical, it is possible to purchase various modifications of the product suitable to various uses. Enterprise will decide which distribution to choose by expectation. Mainly, the expectation is form the load by traffic and by services, it should include. Following table shows the main four distributions and its properties.

Table 1 – Comparison of distributions of MS Windows Server 2008, Source [21].

Edition	Web	Standard	Enterprise	Data centre
Hyper-V virtualization technology	No	Included	Included	Included
Number of instances (physical+virtual)	1	1+1	1+4	Unlimited
Maximum RAM (32-bit)	4GB	4GB	64GB	64GB
Maximum RAM (64-bit)	32GB	32GB	2TB	2TB
Minimum number of CPUs	1	1	1	4
Maximum number of CPUs	4	4	8	64
Hot swap RAM and CPUs	No	No	No	Yes
Cluster Service (failover)	0	0	16	16
Terminal Server	No	Yes	Yes	Yes
Network Access Protection	No	Yes	Yes	Yes
CALs or External Connector required	No	Yes	Yes	Yes

3 REASONS FOR NETWORK SECURITY

The internet opened many opportunities to get information, put information and sell something. In this area there has been no authority controlling the ways of surfing, buying or adding information in. In fact, it is economically impossible. As in Gauss curve here in the world is potential of full variety of particularly minded people. Even developers who know the technology might have reasons for producing the malicious technology against the original technology itself. During the early introduction of the internet, few companies were subject to fraud. However, the number of attack increased and by then people started thinking about the security. It is mainly role of the producers of networking technologies to finance the research for securing the technologies. By now has been made great job and many of threats were put down. It is extremely important for application developers, network designers, and network administrators to be aware of the weaknesses.

While many causes exist for security problems, at least three types of fundamental weaknesses open the door to security problems.

- Technology weakness
- Policy weakness (No written security policy, Lack of disaster recovery plan, No policy for software and ardware additions or changes, Lack of security monitoring, employment policies and internal policies)
- Configuration weakness (Ineffective control lists failing to block intended traffic, default missing or old passwords, Unneeded ports or services left active, user IDs and passwords exchanged in clear text, weak or unprotected remote access through the internet)
- Human weakness[23].

4 COMPANY SECURITY POLICY

The Information Technology (IT) security strategy is one of the main policies, which maintains corporate network safety. This is because couple of reasons. The document has been mandatory to all employees. Legally, employees have signed to follow all of the company’s policies where the network security policy is the part of it. To avoid hacking, enterprises inform their employees of the correct procedures and methods to follow. In addition, the framework and contents of the document should be legally recognised as additional protection in the case of misuse. At time of incorporation, it is mandatory to identify and to document prohibited processes in order to sensitise employees. All employees within all levels of the hierarchy share this responsibility. The document should also define the particular information, which is for company critical. This critical information not only recognises security processes but also the degree of familiarity to which employees require the necessary knowledge to perform tasks such as manufacturing and engineering. By defining the critical information, it is then possible once the critical information is breached to transfer the incident to the law courts for prosecution of the offenders. The policies are uniform for all employees and are used as training material for new-workers and those related to security processes. This is one of two possibilities to maintain awareness during periods of high employee turnover.

4.1 Sample security policy

The security policy is the kind of document, which reflects the company size, internal rules, type of business and the amount of internal information that flows between employees. The following sample illustrates the suggested contents although they may not be applicable to all enterprises. For example, commerce specialising in e-business require more sophisticated and concrete policy.

The fields below reference the topic of particular information. They are not commented as many are discussed in the practical portion of this analysis.

1 Sample Security Policy Outline

2 Introduction

2.1 General Information

2.2 Objectives

3 Responsible Organizational Structure

3.1 Corporate Information Services

3.2 Business Unit Information Services

3.3 International Organizations

3.4 Tenants

4 Security Standards

4.1 Confidentiality

4.2 Integrity

4.3 Authorization

4.4 Access

4.5 Appropriate Use

4.6 Employee Privacy

5 Domain Services

5.1 Authentication

5.2 Password Standards

5.3 Resident Personnel Departure

5.4 Friendly Terms

5.5 Unfriendly Terms

6 Email Systems

6.1 Authentication

6.2 Intrusion Protection

6.3 Physical Access

6.4 Backups

6.5 Retention Policy

6.6 Auditing

7 WEB Servers

7.1 Internal

7.2 External

8 Data Centre

8.1 Authentication

8.2 Intrusion Protection

8.3 Physical Access

8.4 Backups

8.5 Retention Policy

8.6 Auditing

8.7 Disaster Recovery

9 LAN/WAN

9.1 Authentication

9.2 Intrusion Protection

9.3 Physical Access

9.4 Modems

9.5 Dial-in Access

9.6 Dial-out

9.7 Backups

9.8 Retention Policy

9.9 Content Filtering

9.10 Auditing

9.11 Disaster Recovery

9.12 Network Operations Center

9.13 Physical Network Layer

10 Desktop Systems

10.1 Authentication

10.2 Intrusion Protection

10.3 Physical Access

10.4 Backups

10.5 Auditing

10.6 Disaster Recovery

11 Telecommunication Systems

11.1 Authentication

11.2 Intrusion Protection

11.3 Physical Access

11.4 Auditing

11.5 Backups

11.6 Retention Policy
11.7 Disaster Recovery
12 Strategic Servers
12.1 Authentication
12.2 Intrusion Protection
12.3 Physical Access
12.4 Backups
12.5 Retention Policy
12.6 Auditing
12.7 Disaster Recovery
13 Legacy Systems
13.1 Authentication
13.2 Password Standards
13.3 Intrusion Protection
13.4 Physical Access
13.5 Backups
13.6 Retention Policy
13.7 Auditing
13.8 Disaster Recovery
14 Security Services and Procedures
14.1 Auditing
14.2 Monitoring
14.3 Security Incident Handling
14.4 Preparing and Planning for Incident Handling
14.5 Notification and Points of Contact
14.6 Identifying an Incident
14.7 Handling an Incident
14.8 Aftermath of an Incident
14.9 Forensics and Legal Implications
14.10 Public Relations Contacts
14.11 Key Steps
14.11.1 Containment
14.11.2 Eradication
14.11.3 Recovery
14.11.4 Follow-Up
14.11.5 Aftermath / Lessons Learned
14.12 Responsibilities
15 Ongoing Activities
15.1 Incident Warnings
15.1.1 Virus warnings
15.1.2 Intrusion Vulnerabilities
15.1.3 Security Patches
16 Contacts, Mailing Lists and Other Resources
17 References

Table 2 – Sample security policy, Source: William Farnsworth, Sans Institute [1]

5 COMPUTER NETWORK

5.1 Introduction

Computer network is set of computers connected by channels with common communication protocols in order to exchange data. These data flows through many various sets of protocols depend on what media, computing technology, and interface flows. A layer hierarchy was developed in case to understand communication protocols and its encapsulation in each other. Each protocol has its own function. Following paragraph shows how Cisco technologies [15] discuss each layer.

5.2 ISO OSI Model

Layer 1: Physical Layer

The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating network systems. Physical layer specifications define characteristics such as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, and physical connectors. Physical layer implementations can be categorized as either LAN or WAN specifications. Figure 1-7 illustrates some common LAN and WAN physical layer implementations.

Layer 2: Data Link Layer

The data link layer provides reliable transit of data across a physical network link. Different data link layer specifications define different network and protocol characteristics, including physical addressing, network topology, error notification, sequencing of frames, and flow control. Physical addressing (as opposed to network addressing) defines how devices are addressed at the data link layer. Network topology consists of the data link layer specifications that often define how devices are to be physically connected, such as in a bus or a ring topology. Error notification alerts upper-layer protocols that a transmission error has occurred, and the sequencing of data frames reorders frames that are transmitted out of sequence. Finally, flow control moderates the transmission of data so that the receiving device is not overwhelmed with more traffic than it can handle at one time.

Layer 3: Network Layer

The network layer defines the network address, which differs from the MAC address. Some network layer implementations, such as the Internet Protocol (IP), define network addresses in a way that route selection can be determined systematically by comparing the source network address with the destination network address and applying the subnet mask. Because this layer defines the logical network layout, routers can use this layer to determine how to forward packets. Because of this, much of the design and configuration work for internetworks happens at Layer 3, the network layer.

Layer 4: Transport Layer

The transport layer accepts data from the session layer and segments the data for transport across the network. Generally, the transport layer is responsible for making sure that the data is delivered error-free and in the proper sequence. Flow control generally occurs at the transport layer. Flow control manages data transmission between devices so that the transmitting device does not send more data than the receiving device can process. Multiplexing enables data from several applications to be transmitted onto a single physical link. Virtual circuits are established, maintained, and terminated by the transport layer. Error checking involves creating various mechanisms for detecting transmission errors, while error recovery involves acting, such as requesting that data be retransmitted, to resolve any errors that occur. The transport protocols used on the Internet are TCP and UDP.

Layer 5: Session Layer

The session layer establishes, manages, and terminates communication sessions. Communication sessions consist of service requests and service responses that occur between applications located in different network devices. These requests and responses are coordinated by protocols implemented at the session layer. Some examples of session-layer implementations include Zone Information Protocol (ZIP), the AppleTalk protocol that coordinates the name binding process; and Session Control Protocol (SCP), the DECnet Phase IV session layer protocol.

Layer 6: Presentation Layer

The presentation layer provides a variety of coding and conversion functions that are applied to application layer data. These functions ensure that information sent from the application layer of one system would be readable by the application layer of another system. Some examples of presentation layer coding and conversion schemes include common data representation formats, conversion of character representation formats, common data compression schemes, and common data encryption schemes.

Layer 7: Application Layer

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application.

This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication.

Source:Cisco Technologies [15].

6 NETWORK SECURITY

6.1 Overview

Central to the role of server designer and administrator is the concentration on security ratios:

$$\frac{security}{accessibility} \quad or \quad \frac{security}{performance}.$$

The component selected negatively impacts the other. Securing or protecting the corporate network is more question of cost for company. To purchase expensive security services is only one part of the total network security expenses. The more refined or specialised the system, the more time is spent on administration and knowledgebase construction. The importance of securing the network increases due to company policies and the nature of its services in that each will vary. This segment is dividable into two main groups such as, small and medium business delimitating security policies and subsequently, delimitating network security rules.

6.2 Securing small business

A very small business network may constitute an environment wherein hackers have little to read / modify such as, knowledge or other important assets available on electronic processing or storage. It may also comprise as little as one office where there is greater contact between their employees. In both of these instances, one may secure the network with standards as those deployed by advanced home users. A router with its services that include firewall, antivirus, antispyware in each network-connected computer is the minimum for today’s configurations. Security behavioural training is also a valuable part of corporate security and is present in all security-related guidelines. The impact is not limited to networking security only. It affects a very wide range of possible threats. Recent research demonstrates that the percentage of disloyal employees is not small. Seventy-five percent (75%) of companies cited employees as a likely source of hacking attacks. For more details, please consult Attachment I – *Security Statistics*.

6.3 Securing medium enterprises

Once we have to secure a network for a company requiring more security policies (such as, e-business oriented, or with a greater internal network infrastructure, business management software, network data storage, and others) one has to plan seriously to be synchronous and to track related trends. To have a basic notion of which particular rules can be applied to standard policies is to block the services, which are not in use. Then one has to block the ports, which are not in use and block the IP addresses, which could be potentially a risk to connect. The latter are not in use with either our services or host users. Blocking the possibility to connect to the network by host to an unknown physical address, retains claimed user certificates to identification and authentication for access, use of outbound methods of verification.

7 NETWORK SECURITY - PARTICULAR PARTS OF NETWORK

The perception of security in the sense of networking is not consistent with the view it originally evokes. We might envision the network as being a group of cabling, network devices, and rules of communicating. This is only a small part of the components that could be potentially at risk during important information flows. We must however comprehend a network as consisting of cabling, routers, switches, hubs, amplifiers, servers, server configuration as an operating system, network services, and its associated configuration, hosts and its configuration and the individuals with their politics. We therefore, have to focus on the whole ISO-OSI model (section 5.2) and the users who are not included in the network layers model even though they are part of it.

7.1 Cabling

Cabling is the longest route by which data flows. Once the cabling is secured, we determine the transmitting media as well as the physical security in switchboards. Typically, media consists of metallic cable, optical cable, and electromagnetic waves. Within each media, there exists a need to prevent various threats. The easiest prevention occurs with optical cables. There is only the need for physical and encoding security against the transmitting buzz. Optical cables do not deal with electromagnetic compatibility – EMC, or electromagnetic susceptibility - EMS. Opposite to the former are the remaining two types of media. In this case, we have to prevent data encoding, data encrypting and physical security. Today it is popular to secure the wireless networks, as the same threat exists for cabling. Any piece of wire, when used for alternating electric current flow emits electromagnetic waves. Network data flow monitoring uses electromagnetic waves. Hackers then only have to use the right technology for antenna and amplifier. In the case of data flow monitoring it becomes the task for a data encryption system. We also prevent system for buzz in transmitting channel by increasing redundancy.

7.2 Transport layer - network traffic as listenable data

As previously discussed, when metallic cable is used it always remains a potential risk wherein, an intruder may acquire our data. This process was highly used by hackers to obtain this information. Today it is feasible to listen to network data. New developed technologies permit more secured communications. Using old or non-secure services (more for simplicity and availability) such as - POP3, FTP or HTTP protocol we put our data through the network unsecured. We have no difficulties to listen and read pure data from packets. The following example shows how easily the password could be read[1].

```
Headers are omitted.
---------------------------------------------------------------------------
Packet 1
Request command: USER
Request arg: m_seminsky

0000  00 13 f7 eb 9c 15 00 0a  e4 a7 9a 40 08 00 45 00   ........ ...@..E.
0010  00 39 9f d9 40 00 80 06  7b e0 c0 a8 02 64 c3 b2   .9..@... {....d..
0020  58 46 0b 34 00 15 33 50  66 18 bf 71 5d ea 50 18   XF.4..3P f..q].P.
0030  ff df 2e ee 00 00 55 53  45 52 20 6d 5f 73 65 6d   ......US ER m_sem
0040  69 6e 73 6b 79 0d 0a                               insky..
---------------------------------------------------------------------------
Packet 2
Response code: User name okay, need password (331)
Response arg: Password Needed for Login

0000  00 0a e4 a7 9a 40 00 13  f7 eb 9c 15 08 00 45 00   .....@.. ......E.
0010  00 47 d9 7a 40 00 7b 06  47 31 c3 b2 58 46 c0 a8   .G.z@.{. G1..XF..
0020  02 64 00 15 0b 34 bf 71  5d ea 33 50 66 29 50 18   .d...4.q ].3Pf)P.
0030  17 ef 91 ef 00 00 33 33  31 20 50 61 73 73 77 6f   ......33 1 Passwo
0040  72 64 20 4e 65 65 64 65  64 20 66 6f 72 20 4c 6f   rd Neede d for Lo
0050  67 69 6e 0d 0a                                     gin..
---------------------------------------------------------------------------
Packet 3
Request command: PASS
Request arg: heslo

0000  00 13 f7 eb 9c 15 00 0a  e4 a7 9a 40 08 00 45 00   ........ ...@..E.
0010  00 35 9f da 40 00 80 06  7b e3 c0 a8 02 64 c3 b2   .5..@... {....d..
0020  58 46 0b 34 00 15 33 50  66 29 bf 71 5e 09 50 18   XF.4..3P f).q^.P.
0030  ff c0 fc d0 00 00 50 41  53 53 20 6d 61 72 74 69   ......PA SS heslo
0040  6e 0d 0a                                           .....
---------------------------------------------------------------------------
```

Code 1 – unencrypted packets

[1] To be precise – all the headers of other layers are omitted, such as Frame, Ethernet, Internet Protocol and Transmission Control Protocol.

The security solution for password sending is data encryption. The most widespread is the TCP connection without any encryption. A three-way handshake establishment makes TCP connection. This handshaking technique is referred to as the 3-way handshake or as "SYN-SYN-ACK". The TCP handshaking mechanism is designed so that two computers attempting to communicate can negotiate the parameters of the network connection before communicating. This process is also designed so that both ends can initiate and negotiate separate connections at the same time. The following description shows how the connection is established.

- Host A sends a TCP synchronize packet to Host B
- Host B receives A's synchronize packet
- Host B sends a synchronize-acknowledgement packet
- Host A receives B's synchronize-acknowledgement packet
- Host A sends acknowledgement packet
- Host B receives acknowledgement packet. TCP connection is established.

There is not exist a process that deals with encryption in the above. The service for encrypted TCP connection is called SSL – Transport Layer Security. Many might know SSL as Secure Socket Layer, which is the predecessor of SSL. To be more precise, the SSL connection establishes once a three-way handshake and TCP connection. SSL supports mid-layer for the encryprion handshake. The SSL handshake uses a symmetric algorithm such as DES or RC4. A public-key algorithm, usually RSA is used for the exchange of the encryption keys and for digital signatures. The algorithm uses the public key in the server's digital certificate. With the server's digital certificate, the client can also verify the server's identity. The Following description shows how the SSL connection is established.

- “The client sends a client "hello" message that lists the cryptographic capabilities of the client
- The server responds with a server "hello" message that contains the cryptographic method (cipher suite) and the data compression method selected by the server, the session ID, and another random number.

Note: The client and the server must support at least one common cipher suite, or else the handshake fails. The server generally chooses the strongest common cipher suite. The server sends its digital certificate. If the server uses SSL3, and if the server application (for example IIS, Apache, …) requires a digital certificate for client authentication, the server sends a "digital certificate request" message. In the "digital certificate request" message, the server sends a list of the types of digital certificates supported and the distinguished names of acceptable certificate authorities.

- The server sends a server "hello done" message and waits for a client response.
- Upon receipt of the server "hello done" message, the client (the Web browser) verifies the validity of the server's digital certificate and checks that the server's "hello" parameters are acceptable. If the server requested a client digital certificate, the client sends a digital certificate, or if no suitable digital certificate is available, the client sends a "no digital certificate" alert. This alert is only a warning, but the server application can close the session if client authentication is mandatory.
- The client sends a "client key exchange" message. This message contains the pre-master secret, a 46-byte random number used in the generation of the symmetric encryption keys and the message authentication code (MAC) keys, encrypted with the public key of the server. If the client sent a digital certificate to the server, the client sends a "digital certificate verify" message signed with the client's private key. By verifying the signature of this message, the server can explicitly verify the ownership of the client digital certificate.

Note: An additional process to verify the server digital certificate is not necessary. If the server does not have the private key that belongs to the digital certificate, it cannot decrypt the pre-master secret and create the correct keys for the symmetric encryption algorithm, and the handshake fails.

- The client uses a series of cryptographic operations to convert the pre-master secret into a master secret, from which all key material required for encryption and message authentication is derived. Then the client sends a "change cipher spec" message to make the server switch to the newly negotiated cipher suite. The next message sent by the client (the "finished" message) is the first message encrypted with this cipher method and keys.
- The server responds with a "change cipher spec" and a "finished" message of its own.
- The SSL handshake ends, and encrypted application data can be sent.

Here is another protocol which is used to secure the data. It is named TLS –Transport Layer Security. The difference between SSL and TLS is minor. TLS uses stronger encryption algorithms and has the ability to work on different ports. Additionally, TLS version 1.0 does not interoperate with SSL version 3.0.[14]

By defining SSL/TLS protocol functions it is not the finished process of securing by encryption. The SSL protocol provides more posibilities for other services and types of connection to participate. This is why a rectifying message is written above about the right position of SSL/TLS in the OSI model. The SSL/TLS protocol operates above the TCP connection once the TCP connection is established it then turns to establish the TLS connection. After the TLS connection other connections from the application layer such as HTTP which is the main usage may be established. It is important to manage the server configuration so as to have the valid database of trusted certification authorities and valid certificates for data encryption as it expires after a period of time. Once the server configuration is made the HTTP protocol over trusted, encrypted and certified data channel, it is possible to use another name and port number such as HTTPS. The following lists services using secure connection and port numbers.

Table 3 – List of commonly used protocols over SSL/TLS.

Unsecured Name - port	Secured Name-port	Usage
HTTP - 80	HTTPS – 443	Hypertext Transfer
FTP – 20,21	FTPS – 989,990	File Transfer
Telnet – 23	Telnet secure – 992	Remote control
SMTP - 25	SMTP secure – 465*	Mail transfer
IMAP – 143	IMAPS – 993	Mail transfer
POP3 - 110	POP3S – 995	Mail transfer

* Unofficial – the port is shared with CISCO Technologies.

7.3 Switches and Hubs

The switch and hub utilise stronger security for the following reasons. A network hub or repeater hub is a device for connecting multiple twisted pairs or fibre optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. In fact, the hub does not operate with data the amplifying effect is not counted. This type of traffic manager causes collisions and

CSMA/CD process if used very often. It also causes a very high overload of the network bandwidth and services. The successor to the hub is the switch. Switches work at the upper layer – data link layer (Layer 2). It reads the frame header and operates with physical addresses in the network so as not to overload it. It is also possible to find a L3 switch with the L3 is signifying the ability to work at the third layer, which is the same function as the router does. This represents the integration of the switch and the router functions. It is commonly used in home routers where only one interface creates the LAN network and the need for more interfaces, which are used to connect in the same LAN. The switch is used to support this need.

Switch spoofing

When used the first time in the network, it learns all the MAC addresses of each network devices using the ARP exploration request process. It compiles using the ARP table, which is in fact a simple database. Every frame afterwards compares with the database to send it to the right interface at the requesting host. When the network is modified, the switch uses the same exploration request to update its database. Here is the network security risk. In this case, no authority exists confirming the credibility of the data sent to the switch. An attacking host can operate in the LAN network easily by sending the supposititious ARP reply to the ARP question. It then learns the wrong interface number related to some MAC address. By then, the attacker can communicate with the computer, as it is the right end.

Poisoning ARP table

Automatic discovery technology is the part of the directly connected hosts to switch interfaces permits yet another type of spoofing known as spoofing ARP table. This occurs in the LAN environment using the same vulnerability as in the switch spoofing. When the switch discovers and learns the MAC addresses it uses its own database located in its RAM memory. This memory has limited capacity. Therefore, when it sends to the switch too much information for the record it may fail. In this case, some switches cross into an emergency state and switch its function into HUB. It does not require any table to verify results. In this case, the traffic is high causing many collisions. There is the possibility to communicate with each host in the network. The result is about the same for the attacker as with previous case.

Using the poisoning and spoofing

The use is described in the sections above. It is important to know that these cases happen mainly from inside the local area network. This usually represents employees, network rules (mainly MAC address-related assignment of IP addresses) or physical security. The most effective practise in using this is in redirecting all traffic between root input/output and attacker's NIC. By then all of the traffic of the LAN directly leads into NIC and then is resent to the router. A greater response when pinging the other computers in the network is the only indicia. It is also possible to see whether the ARP table is not corrupted by the exact knowledge of all MAC addresses of all hosts, the MAC address of the server's NIC and have possibility to check the table using management tools. These tools are the telnet connection or web based configuration. Of course, these connections are also corruptible. Once this is corrupted, there is no need to think about the more time and knowledge consuming technologies, like spoofing or poisoning. Because the configuration by telnet is discussed later in the router section, we will now deal with web-based connection only.

Configuration by web interface

Configuration based on a web interface is very popular in home use switches and routers as well. The next section on routers deals with enterprise-oriented routers as they do not have web based interfaces, as there is a greater risk possibility and even more maintenance failure risk. A secured web-based connection is made with password authentication. This password is sent through HTTP request for another html page, which is unencrypted as well as from the FTP packet. From previous sections, we have learned about the encryption possibility SSL/TLS. Here is the possibility to encrypt data to have high security during the network transmission. There is another risk, such as key loggers and other technologies to record the password on the host computer. This is discussed later.

7.4 Routers

From The Computer network section, we know that the router is the main device used for structuring and permitting the network to work. The router is responsible for routing the network traffic in particular networks and between each other. Each network has its own settings, such as network settings but also security settings. If we have privileged network of important hosts whose security is privileged we may apply another set of rules than to other networks, which are connected to the same router. If the router does not follow the same level of security as the privileged network, it does not follow the rules as it is configured. The meaning is for password strength, password saving, number of possible connections for maintaining the router, and physical security. We will discuss password security later for hosts in the network. It is important to say that we have some rules in password definition at each security level.

Password strength

A password is “breakable” as with any security technology, but the question is after what period. A strong password might be corrupted after many years by a brute force attack. Passwords like this must be long enough and must contain unusual letters like a combination of small and capital letters, numbers, dots and so. It creates more combinations in attacking the password by brute force. Today the routers have even better practice in password security as it places a delay between password entry and evaluation result if successful or not. Another rule is if the login is, unsuccessful many times it behave differently to disallow the attacker password discovery and even measures information details about the attack.

Password encryption

Another procedure exists when the attacker obtains start-up or running configuration file of router. This may happen, when the attacker is able to log in as a low-level administrator and does not have enough rules to modify router settings. In this case, we use in the router settings the possibility to encrypt the password for saving into memory – configuration file. The password is saved then as a string of hash algorithm results, which is not usable as password. The router has implemented its own hash algorithm based on a random number recalculating. Once the password change is made, the hash algorithm will recalculate the string into hash string to save it directly into configuration file. Once the administrator needs access, he/she fills in the password and the same recalculating process is made. Afterwards it is possible for the router to check the difference between the new hash code and the saved one.

Remote maintaining connections

The number of possible connections for maintaining the router is also very important. It is easy for the network administrator to use some type of remote access, but it decreases the safety. The router can have a modem (AUX) connection in console port, telnet connection for data directly from the network and http protocol based administration connection.

7.5 Hosts

Hosts in the network is meant as all the interfaces which are able to listen and reply to network traffic and do not originally provide network services. These use the network services and this is why it is important to have some computing capable hardware, compatible with the network and application layer protocols. All the hardware is today very similar in compatibility and is developed for more ways of use, to have an easier manufacturing process and more possibilities to remake it to products that are more specific from the IP telephone to high mainframe. This is why it may communicate in the network in a spurious way in the case of the hacker attack. This case is very popular between hackers as it may allow in some way illegal enrichment. A good example is the cash dispenser. It is very complicated to hack a cash dispenser, but very direct in enrichment. Empirical research demonstrates that there are many security rules applied to prevent hacking at the machines.

7.6 Computer vulnerabilities

There are some common computer vulnerabilities as defined by Microsoft [13], which are in fact the most common ones used by hackers today.

Security exploit

A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery that abuse security holes that may result from substandard programming practice. Other exploits would be able to be used through FTP, HTTP, PHP, SSH, Telnet and some web pages. These are very common in website/domain hacking.

Vulnerability scanner

A vulnerability scanner is a tool used to check quickly computers on a network for known weaknesses. Hackers also commonly use port scanners. These verify to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Note that firewalls defend computers from intruders by limiting access to ports/machines both inbound and outbound, but can still be circumvented.)

Password cracking

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to try repeatedly guesses for the password. The purpose of password cracking might be to help a user recover a forgotten password (though installing an entirely new password is less of a security risk, but involves system administration privileges), to gain unauthorized access to a system, or as a preventive measure by system administrators to check for easily *crackable* passwords. On a file-by file basis, password cracking is utilised to gain access to digital evidence for which a judge has allowed access but the particular file's access is restricted.

Packet sniffer

A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

Spoofing attack

A spoofing attack involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.

Rootkit

A rootkit is designed to conceal the compromise of a computer's security, and can represent any of a set of programs, which work to subvert control of an operating system from its legitimate operators. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security. Rootkits may include replacements for system binaries so that it becomes impossible for the legitimate user to detect the presence of the intruder on the system by looking at process tables.

Social engineering

Social Engineering is the art of getting persons to reveal sensitive information about a system. This is usually done by impersonating someone or by convincing people to believe you have permissions to obtain such information.

Trojan horse

A Trojan horse is a program, which seems to be doing one thing, but is actually doing another. A trojan horse can be used to set up a back door in a computer system such that the intruder can gain access later. (The name refers to the horse from the Trojan War, with conceptually similar function of deceiving defenders into bringing an intruder inside.)

Virus

A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Therefore, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. While some are harmless or mere hoaxes most computer virus are considered malicious.

Worm

Like a virus, a worm is also a self-replicating program. A worm differs from a virus in that it propagates through computer networks without user intervention. Unlike a virus, it does not need to attach itself to an existing program. Many people conflate the terms "virus" and "worm", using them both to describe any self-propagating program.

Key loggers

A key logger is a tool designed to record ('log') every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data. Some key loggers uses virus-, trojan-, and rootkit-like methods to remain active and hidden. However, some key loggers are used in legitimate ways. They are sometimes used to enhance computer security. As an example, a business might have a key logger on a computer that was used as at a Point of Sale and data collected by the key logger could be use for catching employee fraud.[13]

7.7 People

A person is surprisingly one of the main topics in network security. Everything we secure, we do against a case of human attack. The norms and values we follow are not that entrenched in the human psyche thus affecting daily decision-making. The East is more religious, societies, and cultures are of a higher context. Therefore, laws are easier to learn and understand. Culture affects everyday life, but still is not enough to cover these thoughts. When companies compete and do not have ideas to be strong competitors they sometimes use unfair business practices to weaken or totally ruin. This depends on the strength of the security rules, how they are applied and the degree of dependency on the internet.

8 COMMON TYPES OF NETWORK ATTACKS

Without security measures and controls in place. Microsoft [12] suggest that the data might be subject to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself.

8.1 Eavesdropping

In general, the majority of network communications occur in an unsecured or "clear text" format, which allows an attacker who has gained access to data paths in the network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on the communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, the data can be read by others as it traverses the network.

8.2 Data Modification

After an attacker has read the data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if it is not required confidentiality for all communications, it is not wanted that the messages to be modified in transit. For example, if you are exchanging purchase requisitions, you do not want the items, amounts, or billing information to be modified.

8.3 Identity Spoofing (IP Address Spoofing)

Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete the data. The attacker can also conduct other types of attacks, as described in the following sections.

8.4 Password-Based Attacks

A common denominator of most operating system and network security plans is password-based access control. This means the access rights to a computer and network resources are determined by who you are, that is, the user name and the password. Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user. When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access later. After gaining access to the network with a valid account, an attacker can do any of the following:

- Obtain lists of valid user and computer names and network information.
- Modify server and network configurations, including access controls and routing tables.
- Modify, reroute, or delete the data.

8.5 Denial-of-Service Attack

Unlike a password-based attack, the denial-of-service attack prevents normal use of the computer or network by valid users. After gaining access to the network, the attacker can do any of the following:

- Randomize the attention of the internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

8.6 Man-in-the-Middle Attack

As the name indicates, a man-in-the-middle attack occurs when someone and the person with whom we are communicating is actively monitoring, capturing, and controlling the communication transparently. For example, the attacker can re-route a data exchange.

When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data. Man-in-the-middle attacks are like someone assuming the identity in order to read the message. The person on the other end might believe it is you because the attacker might be actively replying as you to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack, described later in this section.

8.7 Compromised-Key Attack

A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

8.8 Sniffer Attack

A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunnelled) packets can be broken open and read unless they are encrypted and the attacker does not have access to the key. Using a sniffer, an attacker can do any of the following:

- Analyze the network and gain information to eventually cause the network to crash or to become corrupted.
- Read the communications.

8.9 Application-Layer Attack

An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of the application, system, or network, and can do any of the following:

- Read, add, delete, or modify the data or operating system.
- Introduce a virus program that uses the computers and software applications to copy viruses throughout the network.
- Introduce a sniffer program to analyze the network and gain information that can eventually be used to crash or to corrupt the systems and network.
- Abnormally terminate the data applications or operating systems.
- Disable other security controls to enable future attacks.[12]

II. PRACTICAL SECTION

9 MICROSOFT SERVER 2008 INSTALLATION

The installation of the operating system is now more and more native. It is caused by greater experience of users as well as programmers who care about the ability to install the system in a short time without any extensive interaction with the administrator. Almost all processes are adjustable during the running mode. The only element that decreases the time spent by installation is the hardware maintenance finish. It is therefore important to have all of the hardware connected to the pc before installation begins.

After termination of the installation, we have the chance to set up the network properties. Once the first start of the system is completed, we have to edit a couple of settings to have the computer healthy from the start and keep it updated and secured. The server is up to then not secured, but it is not a high risk as no network services are operational. Once one network service is turned on such as the web server, SQL, mail server, DNS, network printing, folder sharing, we focus on each service keeping it secured. To install Server 2008 we have more choices. . The typical way is to install it from the boot DVD. However, there are more sophisticated ways to do so. This may incorporate usage of the Remote Installation Services and Windows Deployment Services (WDS). They support an enhanced multicast feature when deploying operating system images. WDS is also usable while the network administrators have control over many PCs. While using WDS it is possible to manage various operating systems functions, computer management, local security rules application, creation of audits, software upgrades, systems reinstallation, new programs and features installation. In this thesis, the focus is not on the deployment, as it is not the mandatory topic. The focus concentrates on the standard installation from a DVD as we create the server, which is the first and last point of network management. There is no other server that remotely controls our own server.

10 SYSTEM CONFIGURATION

As said in last chapter, there is couple of functionalities, which are to set up; otherwise, we leave whole system in risk.

Network installation

The network installation is made while the system is installing. The driver for the Network interface card (NIC) is installed with all the other drivers. The protocols such as TCP/IP v 4 and TCP/IP v 6, client of Microsoft network, printer and folder sharing are also installed when the installation is finished. We need to access the network, which is related to the connected NIC to the internet, and configure it by the settings provided from the internet service provider (ISP), such as IP address[2], default gateway, subnet mask and addresses of DNS servers.

Critical security updates installation

As the installation version is rarely the version with the latest updates, patches and service packs, it is strongly recommended to install all the critical security updates, even the less critical ones as well. This is the difference from Unix-like system servers. With servers from Microsoft, administrators have less work with the installation and optimisation of all the critical security updates to the particular servers. With MS Server, it is possible to use the automatic updates, which even makes the system more unmanned. It is also very inexpensive for enterprises as there is less personnel for tasks as in the case of Unix-like systems.

Automatic updates configuration

This action is very simple, because everything is set up. This step accesses the settings and allows the automatic updates process. It is also possible to restart the server while downloading and installing of the updates is done, or to wait for the administrator once the system restart as it may corrupt this important process.

[2] if not assigned automatically. For server connection, we use standard ISP settings where DHCP is not running. For DHCP details see 12.4.

Timing settings

It is also important to set up the local server timing as there are many processes related to timing. All of the log files are saved with time information and by then we can easily browse past actions at the server. By this, we can track vulnerabilities or past attacks. We can reference the attacks, which were done related to security vulnerability. We can even track the time where attacks were not successful using the security path. It is also important to run (if not turned on by default) the timing synchronisation service.

Password policy settings

Creating the password for the administrator follows the same rules used to create passwords for the normal user. The password is created meeting minimum strength rules, which are to set up in local policy settings in

- Enforce password history (msDS-PasswordHistoryLength)
- Maximum password age (msDS-MaximumPasswordAge)
- Minimum password age (msDS-MinimumPasswordAge)
- Minimum password length (msDS-MinimumPasswordLength)
- Passwords must meet complexity requirements (msDS-Password-ComplexityEnabled)
- Store passwords using reversible encryption (msDS-Password Reversible Encryption Enabled)
- Account lockout duration (msDS-LockoutDuration)
- Account lockout threshold (msDS-LockoutThreshold)
- Reset account lockout counter after (msDS-LockoutObservationWindow)

11 THE PHYSICAL NETWORK

For educational and testing purposes, the design of the network is limited. Nevertheless, using the functionality is enough to examine the processes. Some items are virtual, whereas some are simulation. The simulation is based on real processes and has exactly the same functions. The features used as simulation are also used in real networking cases as example, trial version or experimental run. It is often used rather for testing purposes as setting an untried feature into the real system might affect the functionalities of the whole network system in negative fashion. This may cause a total break down of the settings or create an error, which might be difficult to debug.

11.1 Equipment

The following list shows the physical equipment used, from which it is visible that we have used only one server. In the following sections, it is discussed that in reality, situations are important to have physically more machines in case of failure. Many companies use machines that are more physical even for the partition of each network service and they may double or triple. For example, a company offering mail services use web server and database server (others were purposely omitted). As there are forecasted high traffic volumes for the web server as well as the database server, they should operate both servers into its own physical machines. If the company plans, high traffic there is also the need to create alternatives in obtaining the DNS response for users made by more DNS servers each one physically located in a different machine. The IP addresses of all alternative DNS servers are stored in the DNS records of supernal DNS server[3].

- server (32bit AMD Athlon 2500+, 512MB RAM)
- 2 x NIC (100Mbit interface)
- switch
- Connection to the internet (100Mbit/s)
- Patch cables
- domain 4TH Level

[3] Details of DNS services will be discussed later in section 12.3 Domain Name Service - DNS

11.2 Router

As mentioned in the last paragraph there is a type of virtualisation used, which is not used in reality. Once one internet connection is established there is the need to create a new local area network, this problem is solved by adding a router that is capable to set up routing protocol and manage its routing table to set up the range of IP addresses. It is important to note that the equipment list does not contain a router. This is one of the many functionalities of the server to serve virtually created router features with all the settings as normal routers. Normally we should not use a router virtually in the server as it causes an efficiency decrease. Routing does not represent the minority portion of computer time. This is why most of companies purchase routers as a solo machine as de facto contain all of the ordinary pc features. There is a difference in that there is a non-intensive requirement to compute all the requirements from the operating system of the universal server (for example, MS Server 2008). There is an operating system with limited functionalities to satisfy the conditions to manage the high-speed routing. The network performance rapidly decreases using the server as router, but for our purposes, it is still sufficient, as we are not testing any high bandwidth and low latency requiring features.

11.3 Server

The main arithmetic logic unit in our networking is the server as a physical machine. We have used standard computer with the Microsoft Server 2008 installation. For having full capabilities, it is important to have some routing possibilities as a virtual service. For doing this, we decided to add another NIC card into machine. The server’s power management is made by over-voltage protection and the back-up power supply for this simultaneous operation for at least one hour. This is done by battery.

11.4 Switch

As we have already seen, the switch supports the function of being in the middle of a single wired network with particular connections at hosts or servers side. It does not create a new network as it interconnects all of the interfaces and permits them to work together in one network. It allows the network to work without the collisions by switching the particular Ethernet frames by using MAC addresses table.

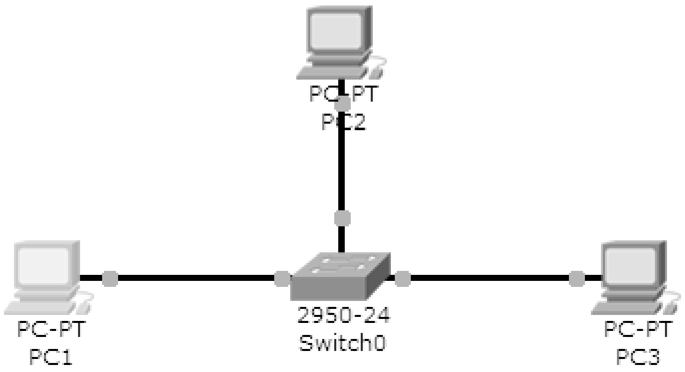


Figure 1 - Schema of standard switch interconnection

11.5 Connection to the internet

There is a connection for the internet made by the interface of the university router. Connection settings follow:

- The IP address 195.178.89.12
- The subnet mask is 255.255.255.0
- Default gateway 195.178.89.1
- Primary DNS server 195.178.88.66
- Alternative DNS server 195.113.144.233

Cat. 5 UTP patch cable makes the connection and the Fast Ethernet interface connection. The connection has a bandwidth of 100Mb/s.

11.6 Patch cable

The cabling is an integral part of the networking. There are many rules to establish such as, the physical part of the network that include: the type of cabling, type of interconnections, types of end of cables, maximum length of cabling, building infrastructure with switches, routers, building the wireless, power over Ethernet, Ethernet over power cables, location of switch room, physical security of switch room, etc. We have focused on a very small part, as the other parts listed above are not obligatory with the current discussion.

A patch cord, patch cable (also called a pigtail) is an electrical or optical cable, which is primarily used for interconnection of two devices from network. These are called especially because there are not only cables in network, but these PC users know the most. RJ-45 connector usually ends these cables. They have many different colours to be easily distinguishable, and are no longer than 5m. The patch cables from type of wiring are two types. Each type is used for another connection. One type is straight through. This cable is used for interconnecting between network intermediary devices to hosts, such as PC to Switch, PC to router, Switch to Router, Server to switch. The second type is the crossover cable. The crossover type is used in the connection between two types of network devices, like the intermediary to the intermediary or the host to the host. The solution to solve the electrical wiring is to use each of the ANSI standards. The two standards are ANSI/TIA/EIA-568A and ANSI/TIA/EIA-568B. However, we can also find commercial brands with T568A and T568B, which essentially is the same.

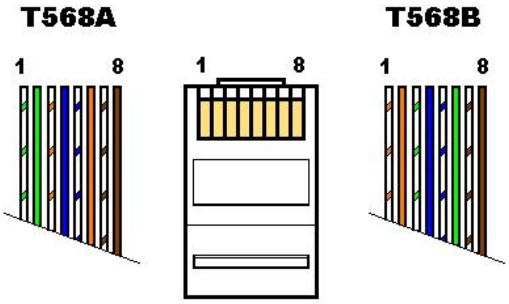


Figure 2 - Wiring of each standard

To create straight-through cable means to connect each end with a different standard (T568A - T568B). To create cross over cable – connect both ends with the same standard (T568A - T568A).

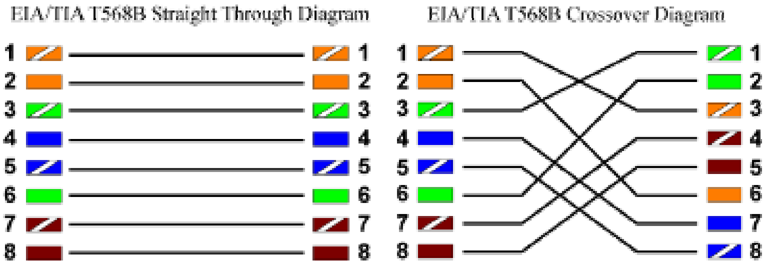

EIA/TIA T568B Straight Through Diagram
EIA/TIA T568B Crossover Diagram
1
2
3
4
5
6
7
8

Figure 3 - Wiring of each standard

We have used the straight connection to the server, which is not the patch cable. This is 100BaseT type of Ethernet connection. This is the Category 5 UTP cable with 100Mb/s and 100m maximum of length. The other connection is between the LAN intermediating interface and switch. For this connection is important to follow the parameters which we have from the other interface as 100Mb/s. Therefore, we have used the same patch cable and straight-through wiring as seen in Figure 2 and Figure 3.

11.7 Network schema

For demonstrational purposes, we have used a simple one-branch office. In this branch we can have up to 255 PCs, keep to the IP design of the network. The number of PCs is not relevant from the Figure 2. Number of interfaces of the switch limits it. We can even use more switches in the way. However, there is important to take care about the network understanding, as some switches might not support redundant routes or cascade of switches to increase the number of interfaces used for connection of PCs. As you can see, the server has the two network interfaces. The one is interconnecting server with internet and the other with LAN. This kind of schema is one of the security solutions to keep our LAN under firewall and NAT[4].

[4] NAT and Firewall is discussed later in *12.2 Network Address Translation - NAT* and *12.5 Firewall - WFAS*.

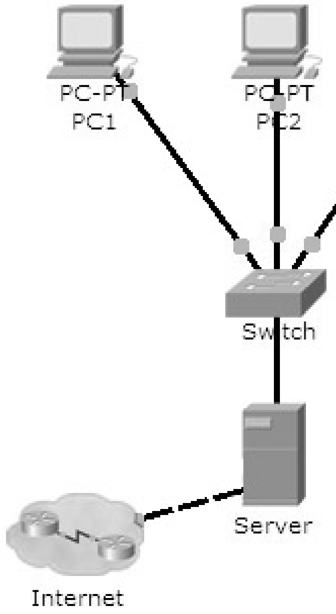


Figure 4 – Physical schema of the network

11.8 IP design of the network

The solution to the IPv6 problem is the limited capacity of the maximum number of used IP addresses. The step forward in saving the internet infrastructure is to find the privately based LAN addressing. The IANA organisation finds the address ranges of 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255. These addresses are not in public use. The latter are not able to travel through internet. This is why the number of computers connected to the internet could be dramatically increased. To be more precise – the number of computers connected to the internet by public IP address remains the same, but it allows proxy creation or NAT router technologies. They translate the IP addresses from private ones into public using port to IP address translation. This has increased the number of possible connections to the internet in total as each IP address can have more ports (65535). Therefore, at one public IP address, it is now more popular to run more connections from other computers in one LAN network. [5]We have assigned following design of IP addresses:

- the IP adress range for hosts is 10.0.0.2 – 10.0.0.255
- the IP adress for gateway is 10.0.0.1
- the IP adress for network is 10.0.0.0
- the IP adress for broadcast is 10.0.0.255
- the subnet mask is 255.255.255.0
- the IP adress of the WAN interface is 195.178.89.12
- the subnet mask for WAN network is 255.255.255.0

Following figure demonstrates the IP design as listed above.

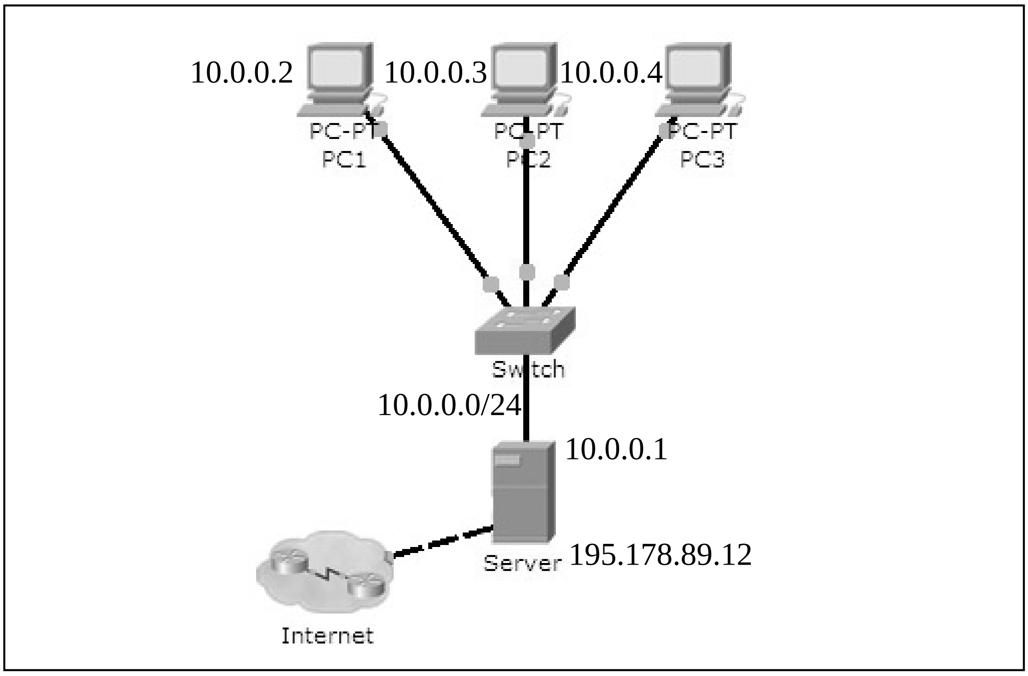


Figure 5 – IP model of the network

[5] The soltuion is the IPv6, which allocate more than one billion IP addresses for one square centimetre of the Earth surface. The number of combinations we can have from IPv6 addressing is $16^{32} = 3.4\times10^{38}$.

12 USED SERVICES

Network services is one of the main topic of this thesis. The services installed and configured solves all of the functions we have to have in case of scalable, functional, automatic network with security rules disallowing unwanted connection in the internet. We had to install the minimum of routing, NAT, domain, DHCP, firewall, SSL, IIS, https, php and sql. In following paragraphs there is short description of each service listed above. Please note that installing and allocating the services is rarely process of folding services It does not matter what sequence we use. Although there may be recommended procedures to complete final configuration.

12.1 Routing

Routing is the act of moving information across an internet from a source to a destination. Along the way, at least one intermediate node typically is encountered. Routing is often contrasted with bridging, which might seem to accomplish precisely the same thing to the casual observer. The primary difference between the two is that bridging occurs at Layer 2 (the link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer). This distinction provides routing and bridging with different information to use in the process of moving information from source to destination, so the two functions accomplish their tasks in different ways. The topic of routing has been covered in computer science literature for more than two decades, but routing achieved commercial popularity as late as the mid-1980s. The primary reason for this time lag is that networks in the 1970s were simple, homogeneous environments. To enable routing at MS Server 2008 go to the server manager, select the roles of server. Press add role. Follow the wizard as follows – select next in table before you add role, in tab select server roles, tick the box next to Network Policy and Access Services role, then press next, on the next wizard page, select Routing and Remote Access Services (RRAS) to install two role services, Remote Access Service and Routing. By clicking next and finish, then after restarting the server, we have the routing service running. The way in which we use routing in our laboratory is to define and logically create the local area network and distribute traffic in between the internet and LAN. The routing in MS Windows 2008 works under Network Policy and Access Services – Routing and Remote Access (RRAS) Label as shown in following figure. The main settings is listed in each type of IP(4/6) menu. There we can find general settings for each interface such as multicast heartbeat and multicast boundaries. Static routes are the type of routing characterised by the absence of communication between routers regarding the current topology of the network. This is achieved by manually adding routes to the routing table. The opposite of static routing is dynamic routing named as *General*. NAT is the function listed in paragraph below. IGMP - The Internet Group Management Protocol is a communications protocol used to manage the membership of Internet Protocol multicast groups. IP hosts and adjacent multicast routers to establish multicast group memberships use IGMP.

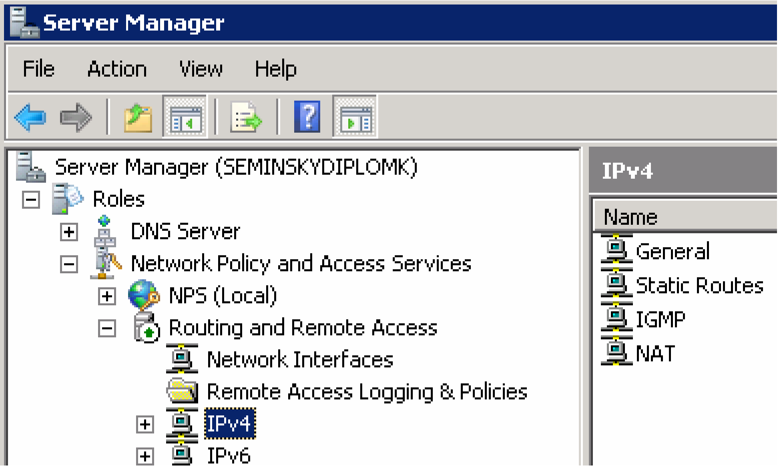

Server Manager
File
Action
View
Help
Server Manager (SEMINSKYDIPLOMK)
Roles
DNS Server
Network Policy and Access Services
NPS (Local)
Routing and Remote Access
Network Interfaces
Remote Access Logging & Policies
IPv4
IPv6
IPv4
Name
General
Static Routes
IGMP
NAT

Figure 6 – settings of routing in server manager

Configuration

Once the installation finishes, we open the Routing and Remote Access console from Administrative Tools, right-click on the local server and select Configure and Enable Routing and remote Access. This launches the Routing and Remote Access Server Setup Wizard; select Network Address Translation (NAT) on the Configuration page of this wizard. Next, on the NAT Internet Connection page, we select the network interface that is on the Workplace LAN, which is the "public interface" of the NAT router. The next page asks us whether the NAT router should also provide DHCP and DNS services to the computers on the Test network, which is connected to the "private interface" of the NAT router. Since our client computers all have static IP addresses assigned, we will choose not to do this. Once the wizard finishes, the RRAS service starts up. Then it is configured for both IPv4 routing and NAT as well. To see this, we can begin by right clicking on the local server in the RRAS console and selecting Properties. The General tab shows that IPv4 routing has been enabled, which means IPv4 packets can be forwarded from one NIC to the other. Selecting the NAT node in the RRAS console shows that three network interfaces were created when NAT was configured on the server using the Routing and Remote Access Server Setup Wizard. Figure 10 shows the properties of Local Area Connection, which in this scenario is the network connection to the Test (10.0.0.0) network. Note that NAT considers this network the "private" network, that is, the network "behind" the NAT router. Properties of Local Area Connection 2, are in this scenario the network connection to the Workplace (195.178.89.12) network. Note that NAT considers this network the "public" network, that is, the network "in front of" (on the Internet side of) the NAT router.

Common threat - default password

Very common vulnerability is at home network users who could be vulnerable to attacks from hackers who can alter the configuration of a broadband router or wireless access point. There are many various cheapest equipments such as routers. These are commonly used by users having not very much knowledge about networking and by this knowledge about possible threats. Each low-cost router allows straight after turning on the network running without any configuration. If so, there is no need for long configuration to let the routing service run. People sometimes do not think it is important (or do not know how to do so) to change password in their router. Therefore, there is a default password saved for connecting the router settings through web interface. This vulnerability is for professionals underestimated, as there are many routers around the world with default password. It is even not complicated to setup searching-bot for these routers.

Prevention

Prevention is apparent – to let people know about the importance in manual and let them always set the password.

12.2 Network Address Translation - NAT

In computer networking, network address translation (NAT) is the process of modifying network address information in datagram (IP) packet headers while in transit across a routing device for the purpose of remapping a given address into another. By this process, NAT allows to share a connection to the public Internet through a single interface with a single public IP address. The computers on the private network use private, non-routable addresses. NAT maps the private addresses to the public address. Translation is a useful feature that adds diversity and security to a network in a small to medium sized enterprise[6]. With the advent, and implementation, of IPv6 still in its beginning stages, we can expect to see NAT used for many years to come or forever with the security purposes.

The settings are easy to set, but it needs of course the knowledge of our networking and access policies. For this cases there is possible to set up some features such as dynamic IP address pool and static IP address pool. For the pools, we can assign as many ranges of IP addresses as we wish. We have assigned the NAT IP address pool for our private network. All the host IP addresses from range 10.0.0.2 to 10.0.0.255 are able to communicate through our proxy server at port.

- IP address range 10.0.0.2 to 10.0.0.255
- ports: 80(HTTP), 443(HTTPS), 1723(VPN)

Ommiting any IP addresses from the IP address pool have security effect as these addressess are not able to have sent, neither receive packet any further off the local network.

Installation

As we installed from configuration wizard of routing installation, we have also installed the NAT server. We have set up server as NAT router. The primary installation of NAT means the installation of the router first wherein the NAT service is configured. In case of a manual installation, we deploy a similar process as that for the NAT routing installation. On Server Manager we press add roles, and then we have to have ticked on the Network Policy and Access Services as well as the Routing and Remote Access. Then we tick on NAT service. Then we press install and restart the machine after finishing the installation.

Configuration

The NAT configuration takes place from Server Manager – Roles – Network Policy and Access Services – Routing and Remote Access – Ipv4 – NAT and is made by the interface selection and the settings assignment related to selected interface. After selecting the

[6] For precise NAT example see internet page on Microsoft Technet: http://technet.microsoft.com/en-us/library/cc754802%28WS.10%29.aspx

particular interface that we wish to configure, the properties window is launched giving the option to change settings such as packet filtering and port blocking, as well as the enabling/disabling certain features, such as the firewall. We are able to select the interface type – to specify what the network connection will be the connection with LAN created by router and which one will be connected to the internet. We establish NAT for the interface connected to the internet.

12.3 Domain Name Service - DNS

Most of the internet connections are made primarily using the Domain Name Service (DNS). These services are responsible for the naming of the computers in the network through public-usable names that are easily understood or remembered. All the computers on the internet have their own IP address. This is the only vector for usage. We are used to domain names that are each time resolved as IP address. This is performed by DNS service operating on the servers. There is a hierarchy of DNS servers as shown below. The main organisation who runs the background of the internet such as root DNS servers is IANA[7]. The Following figure depicts the hierarchy by domain sema.fai.utb.cz and what servers are contacted in the fourth level and higher domains. Each box represents at least one domain controller or DNS server.

[7] The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. For details see http://www.iana.org/

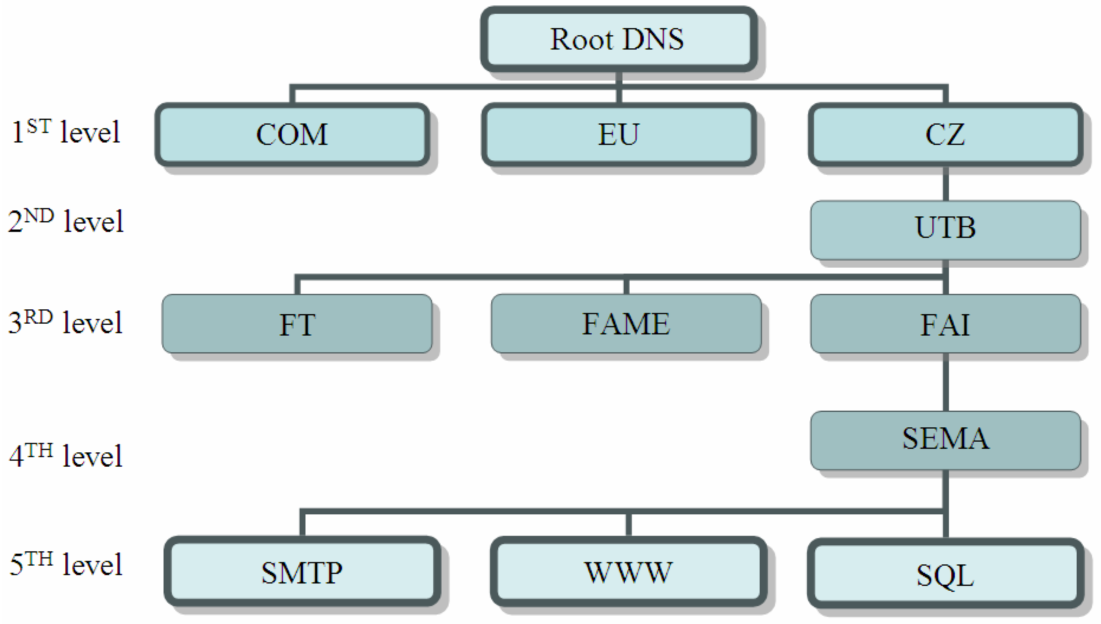


Figure 7 – sample diagram of DNS hierarchy

Installation

The installation starts the same as other network services or in the server role.

- From the Start menu, select - Control Panel - Administrative Tools - Server Manager.
- Expand and click Roles.
- Choose Add Roles and follow the wizard by selecting the DNS role.
- Click Install to install DNS in Windows Server 2008.

After installing DNS, we can find the DNS console from Start - All Programs - Administrative Tools - DNS. Windows 2008 provides a wizard to help configure DNS.

Configuration

When configuring our DNS server, we must be familiar with the following concepts:

- Forward lookup zone
- Reverse lookup zone

A forward lookup zone is simply a way to resolve host names to IP addresses. The forwarding lookup zone is the DNS records pool where the DNS server is authoritative for the particular DNS namespace. A typical example of DNS records in the forwarding zone is illustrated by the following[8]:

```
domain.cz         A        81.2.194.136
local.domain.cz   A        127.0.0.1
domain.cz         MX       10 mx.domain.com
pop3.domain.cz    CNAME    pop3.domain.com
```

Code 2 – list of typical DNS records

A reverse lookup zone allows a DNS server to discover the DNS name of the host. It is the exact opposite of a forward lookup zone.

A **reverse lookup zone** is not required, but it is easy to configure and will allow for our Server to have full DNS functionality. A Standard Primary zone stores the database of DNS records in a text file. This kind of text file is or can be shared with the others DNS services which information is stored also in text file. These DNS servers are called secondary DNS servers. These are synchronised once the set-up period finishes and if the number of changes in DNS record is different in the primary DNS server. Finally, a Standard Secondary zone creates a copy of the existing text file from the primary DNS server. We use secondary servers as the backup servers, which are alternatively in use in case of a malfunction of the primary or if DNS server traffic is, high and we are using the load balancing process between them.

To open the DNS server configuration tool:

- select DNS from Roles in Server Manager.
- right click and choose Action - Configure a DNS Server
- Click Next and choose forward lookup zone
- Select server is maintaining the zone instead of ISP.
- Click Next and type the name of the zone you are creating (the zone is the domain we have rights to add higher domain).
- do not allow dynamic updates when you set up primary DNS
- Choose that you want an IPv4 DNS.
- Click Finish.

[8] For list of all possible DNS records see reference [16] List of DNS record types.

To Manage DNS records, we have now installed and configured the DNS server, and are ready to add records to the zone(s) created. There are various types of DNS records available with the commonly used DNS records[9] being:

- Start of Authority (SOA)
- Name Servers
- Host (A)
- Pointer (PTR)
- Canonical Name (CNAME) or Alias
- Mail Exchange (MX)

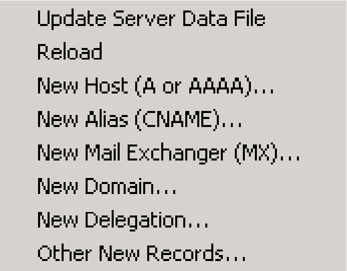


Figure 8 – list of possible DNS records as a right click to particular forward lookup zone

The Start of Authority (SOA) record is the always the first DNS record. The Start of Authority (SOA) tab allows us to make any adjustments if necessary, such as changing the configuration without deleting the DNS zones and the wheel recreation, changing the administration rights for DNS and changing the primary server holding the SOA record. The Name Servers specifies all of the name servers for a particular domain. We set up all primary and secondary name servers through this record.

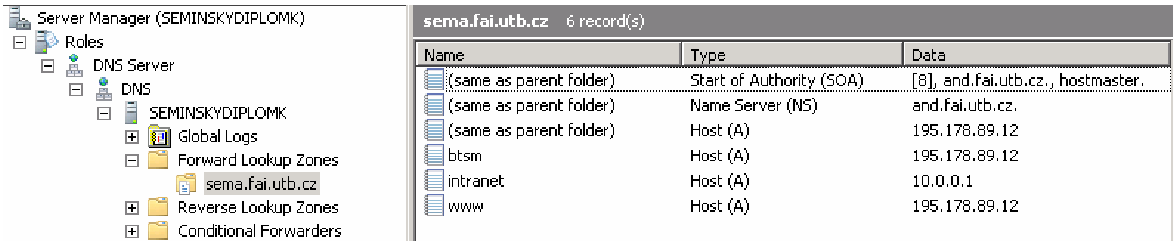
To create a Name Server, we can follow these steps:

- select DNS from Roles in Server Manager.
- Expand the Forward Lookup Zone.

[9] The example of exact DNS records may be found above in Code 2 – list of typical DNS records

- Right-click on the appropriate domain and choose Properties.
- Select the Name Servers tab and click Add.
- Enter the appropriate FQDN Server name and IP address of the DNS server we want to add.

We assign several DNS records such as, MX and A. The following list shows the exact records attached to our server.



sema.fai.utb.cz 6 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[8], and.fai.utb.cz., hostmaster.
(same as parent folder)	Name Server (NS)	and.fai.utb.cz.
(same as parent folder)	Host (A)	195.178.89.12
btsm	Host (A)	195.178.89.12
intranet	Host (A)	10.0.0.1
www	Host (A)	195.178.89.12

Figure 9 – The DNS records in our server

Common attack – DNS Cache poisoning

DNS Cache poisoning is one of the critical vulnerabilities to the entire internet. The DNS service generally uses open architecture, so there is possibility of attack in many ways. This attack may be caused by an improper design of the DNS server configuration, not having been updated the DNS software at the ISP level. Normally the DNS resolves the IP address from the domain name by asking the DNS servers, as described previously , from the root DNS servers to the local ones. In case of decreased DNS traffic through the internet a process that allows for records catching for a period of time after a DNS answer is in use. This caching process may be corrupted and the ISP may provide malicious information about IP addresses related to domain names. The result of this issue is a malicious but identical web site as in the case of Internet banking wherein the site scans the password while the user logs in to what is assumed to be a trusted web site. This vulnerability is known under number VU#800113 at the US-CERT organisation. For details, please consult Vulnerability Note VU#800113 [22].

Prevention of DNS poisoning

As a preventative measure, network administrators must avoid DNS poisoning by updating the latest patches to the DNS software and even the server operational software itself. The second part of prevention is that people accessing highly trusted websites such as internet banking should know about the HTTPS certification and be able to check that there is not downloaded malicious website[10], in case of new process to compromise the DNS cache at ISPs. The most user- friendly technology is DNSSEC. It allows a secured communication between the DNS hierarchy servers. If the system should run on all DNS servers, there is less possibility to obtain faulty or inappropriate information. The DNSSEC uses the standard mathematic algorithms like RSA and certificate with certification authority. Details of DNSSEC are not discussed in this thesis, but details regarding SSL and certification methods are available in section 12.7.

12.4 Dynamic Host Configuration Protocol - DHCP

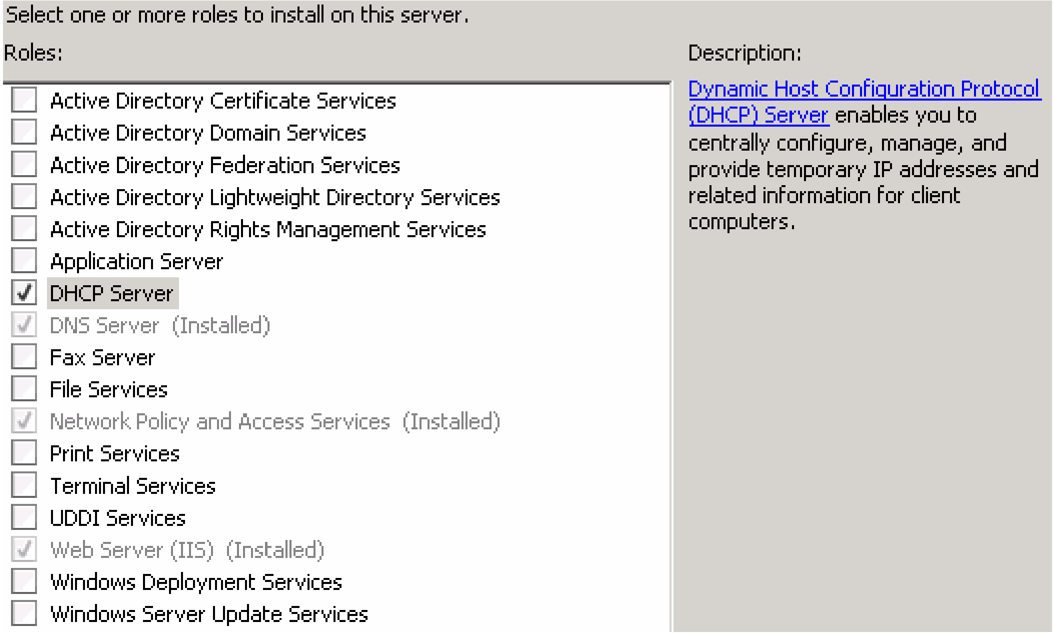
Dynamic Host Configuration Protocol (DHCP) is used when we want to send to hosts who listens the DHCP port, common dynamic or static data related to the network. The service is core infrastructural service for networking and provide very easy host configuration without any knowledge of network parameters or way to set up the network parameters related to getting access into network. DHCP is one of network security engines that run with many various data to send such as Basic options, IP host options, IP interface options, Link layer options, TCP options, Application layer options, NetBIOS over TCP/IP options, Vendor-specific options, User class options, DHCP extensions, Administrator-defined options, and Microsoft options. For example, we can use it when we want to assign the IP addresses to hosts in network automatically. DHCP is mainly used when there is no static assignation of IP addresses in the network.

Installation

The installation is in following few steps:

- sellect roles in server manager
- press add role
- sellect DHCP
- configure the scope
- press install
- restart server

[10] As discussed below in detail, section 12.7.



Select one or more roles to install on this server.

Roles:

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☑ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ☐ File Services
- ☑ Network Policy and Access Services (Installed)
- ☐ Print Services
- ☐ Terminal Services
- ☐ UDDI Services
- ☑ Web Server (IIS) (Installed)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

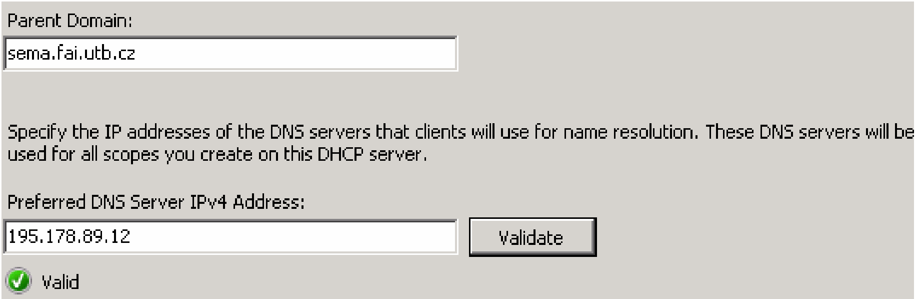
Description:

Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.

Figure 10 – selecting the role of DHCP server for installing

Configuration

The configuration is a part of installation. Once we finish the installation, we have to set-up the server with the entire configuration. The configuration is made initially by setup wizard that is easy to use. At this point, we will begin being prompted for IP network information, scope information, and DNS information. If we only want to install DHCP server with no configured scopes or settings, we can click Next to skip the questions and proceed with the installation. On the other hand, we can optionally configure our DHCP Server during this part of the installation. In our case, we chose to take this opportunity to configure some basic IP settings and configure our DHCP Scope.



Parent Domain: sema.fai.utb.cz

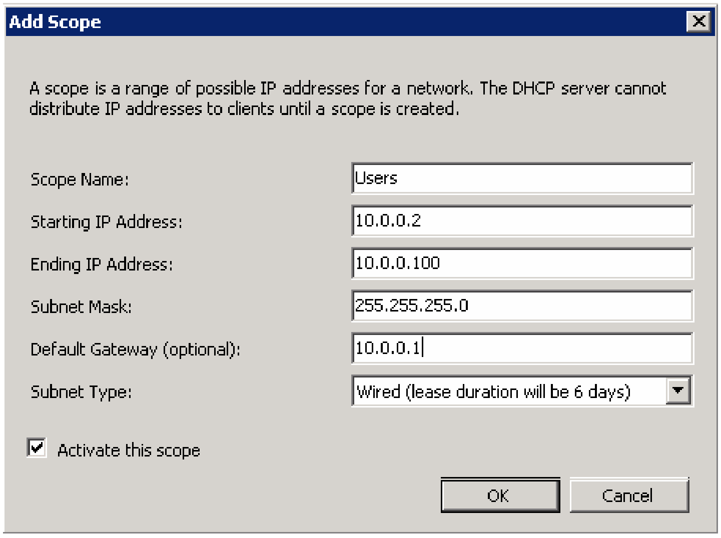
Specify the IP addresses of the DNS servers that clients will use for name resolution. These DNS servers will be used for all scopes you create on this DHCP server.

Preferred DNS Server IPv4 Address: 195.178.89.12

✓ Valid

Figure 11 – adding domain and DNS server

Next, we have to enter the Parent Domain (sema.fai.utb.cz), Primary DNS Server (195.178.89.12), and Alternate DNS Server (none yet) and click Next. Then we were prompted to create some scope that refers to scope of IP addresses as listed below. There is scope of IP addresses defined by starting and Ending IP address. Note that this scope of IP addresses must match the IP addressing rules by subnet mask. For example, it is not possible to assign scope of IP addresses from 10.0.1.0 to 10.0.2.0 with the subnet mask 255.255.255.0. The scope can be assigned only to IP addresses from the host part of IP address.


Add Scope

A scope is a range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created.

Scope Name: Users
Starting IP Address: 10.0.0.2
Ending IP Address: 10.0.0.100
Subnet Mask: 255.255.255.0
Default Gateway (optional): 10.0.0.1
Subnet Type: Wired (lease duration will be 6 days)

☑ Activate this scope

Figure 12 – DHCP scope configuration

After confirming the installation details and clicking install, we have done the installation. There is also need for restart the computer. For further configuration or checking the performance, we go to the server manager and click DHCP in server roles.

12.5 Firewall - WFAS

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices that is configured to permit or deny computer based application upon a set of rules and other criteria. Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.[17]

Windows Firewall with Advanced Security (WFAS) is implemented with new architecture. It allows windows users to be eligible to authorise their own traffic through an authentification process made in firewall. This kind of firewall is named host-based firewalls. The host-based firewall is built in to Windows, is already installed, now has more features, and is now easier to configure in compare to previous releases. In addition, it is really one of the best ways to secure a crucial infrastructure server. The new features are new GUI interface, Bi-directional (inbound and outbound traffic filtering), works with IPsec, Advanced Rules configuration (it is possible to create rules for Windows Active Directory (AD) service accounts & groups, source/destination IP addresses, protocol numbers, source and destination TCP/UDP ports, ICMP, IPv6 traffic, and interfaces on the Windows Server).

NAT and the basic firewall option have also been enabled. The inbound and outbound buttons will open a window that will allow restricting the traffic based on IP address or protocol packet attributes. As per instructions, certain TCP packets are dropped before they reach the client computer. Thus, making the network safer and giving to us more functionality. This is useful if, for example, we wanted to reject all packets coming from a blacklisted IP address or restrict internal users access to port 21 (ftp).

Configuration

The configuration of WFAS we find traditionally in server manager under configuration - Windows Firewall with Advanced Security. There is possible to find inbound rules, outbound rules, connection security rules, monitoring, and WMI control. For preparing the configuration, we should follow at least steps listed below.

- Identify the protocol we want to filter
- Identify the IP address (source and destination), port number (source and destination)
- Identify the program we want to let it connect the internet
- Identify whether we need to use IPSec protocol or authenticate users in firewall
- Identify what users profile should be applied for

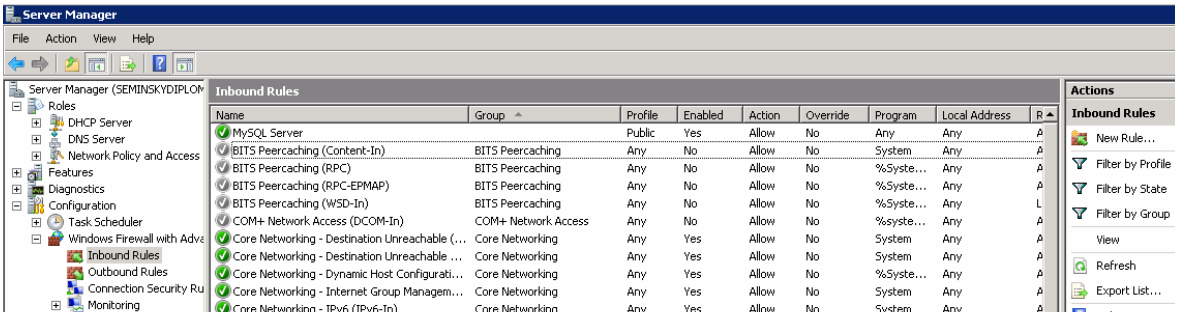
To add a rule to the firewall we identify the following:

- Protocol HTTP
- All range of IP addressess, source port number all, destination port number 80

- Program Apache
- no IPSec/user authentification needed
- all profiles

In the case of HTTP traffic configuration allowed through Apache that is a very popular HTTP server, we follow steps described above. In the case of using IIS (Internet Information Services) which is a Microsoft product, it is easy to install the product as a service. This product automatically adds the rule to the firewall and other settings. It is possible to change some security settings from the settings panel in IIS. However, for some reasons it is complicated to manage if unusual requests are planned. To create the rule for Apache server to send and receive HTTP requests we follow these rules:

- Click in server manager configuration – Windows Firewall with Advanced Security – inbound rules
- On the right row click New Rule…

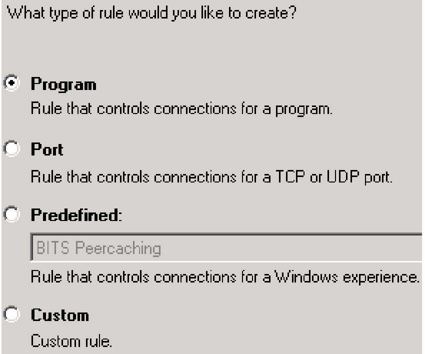


Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	R
MySQL Server		Public	Yes	Allow	No	Any	Any	A
BITS Peercaching (Content-In)	BITS Peercaching	Any	No	Allow	No	System	Any	A
BITS Peercaching (RPC)	BITS Peercaching	Any	No	Allow	No	%Syste…	Any	A
BITS Peercaching (RPC-EPMAP)	BITS Peercaching	Any	No	Allow	No	%Syste…	Any	A
BITS Peercaching (WSD-In)	BITS Peercaching	Any	No	Allow	No	%Syste…	Any	L
COM+ Network Access (DCOM-In)	COM+ Network Access	Any	No	Allow	No	%syste…	Any	A
Core Networking - Destination Unreachable (…	Core Networking	Any	Yes	Allow	No	System	Any	A
Core Networking - Destination Unreachable …	Core Networking	Any	Yes	Allow	No	System	Any	A
Core Networking - Dynamic Host Configurati…	Core Networking	Any	Yes	Allow	No	%Syste…	Any	A
Core Networking - Internet Group Managem…	Core Networking	Any	Yes	Allow	No	System	Any	A
Core Networking - IPv6 (IPv6-In)	Core Networking	Any	Yes	Allow	No	System	Any	A

Figure 13 –network rules configuration in windows firewall - server manager.

- Choose Program in table of types of rules



What type of rule would you like to create?

● **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

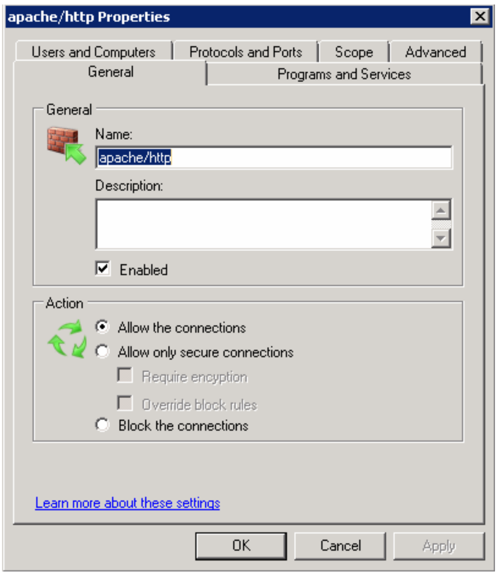
○ **Predefined:**
BITS Peercaching
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Figure 14 – types of rules

- After clicking next we assign the path to the program which should be allowed to connect the internet

- Check the box to allow the connection either if it is secure or not[11]
- Check all boxes to apply the rule for Domain, Private and Public as well.
- Then we should add the name and description which will be used in showing the rule in table of rules. So we can add APACHE/HTTP and no description is needed as this rule is very typical.
- After clicking finish we have added a simple rule to WFAS.
- After doubleclick the rule we can easily change all the settings.



apache/http Properties

General

Name: apache/http

Description:

☑ Enabled

Action

● Allow the connections

○ Allow only secure connections

□ Require encyption

□ Override block rules

○ Block the connections

Figure 15 – settings for the rule after double-click

12.6 Web server - IIS

The web server is only a presentation utility used in the interaction between internet user and our company. All companies should today have some sort of internet commercial presentation . To have secured this presentation is important as many hackers can perform an unwarranted action. They can change the information by its meaning or by deletion. In addition, they can monitor the password information, credit card number from online paying gate or any other sensitive recorded data. All of this is very unwanted but leaving the system secured decrease performance. We always deal with ratio of performance and

[11] As HTTP protocol should be very open and no restriction should be added to it. Protocol 80 is listenable

security. A Web server in technical means is a kind of application (application layer protocol[12]) that delivers (serves) content, such as Web pages, using the Hypertext Transfer Protocol (HTTP), over the World Wide Web. The HTTP service is a host-server based service and runs in the steps listed below.

- Web server is running
- Web server has attached the file to deliver in case of request
- Client application from any host in the internet send HTTP request to server
- Server listens at the port 80 to read the request
- Server get the request (source address and port number included)
- Server touch the information about which file to send back[13]
- Server sends the file to the client application using the destination IP address and port number based from source IP address and port number from the request packet.

Note: TCP session and DNS requests were omitted as we explain only the web server function.

For example, here we can see the typical HTTP request and response.

for server only for http requests and no other services. This setting disallows the IPSec authentication.

[12] For details see section 5.2 ISO OSI Model

[13] Usually it is the HTML, PHP, ASP file located in main www root folder. (Usually named INDEX.PHP)

```
HTTP REQUEST:
=============
GET http://www.sema.fai.utb.cz HTTP/1.1
User-Agent: Mozilla/5.0 Gecko/20040803 Firefox/0.9.3
Accept-Charset: UTF-8,*

HTTP RESPONSE:
=============
HTTP/1.0 200 OK
Date: Fri, 15 Oct 2004 08:20:25 GMT
Server: Apache/1.3.29 (Unix) PHP/4.3.8
X-Powered-By: PHP/4.3.8
Vary: Accept-Encoding,Cookie
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
Content-Language: cs
Content-Type: text/html; charset=utf-8
<html><body>
```

Code 3 – HTTP request and response example

We have various possible applications, which can be run at the server machine to run web server. The typical ones are Apache, Microsoft IIS and others that are minor as we can see from Table 4.

Table 4 – list of web servers in order of usage. Source: Netcraft [18].

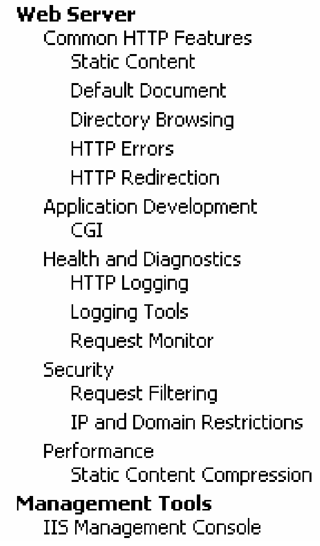
Developer	Usage - January 2010	Percent
Apache	111,307,941	53.84%
Microsoft	49,792,844	24.08%
Nginx	15,568,224	7.53%
Google	14,550,011	7.04%
Lighttpd	955,146	0.46%

As we have seen, there are more possibilities to install web server. The reasonable possibility is to install on Microsoft Server the Microsoft IIS. The reason is we have settings compounded in a common interface called Server Manager. The application is implemented in all ways due to the complex definition of the security rules such as the domain controller settings, firewall, active directories, and others.

Installation

The installation is the easiest part of having web server. To install the IIS web server we may follow these steps:

- Launch server manager
- Click add-rule
- In table of choosing the rule we choose IIS
- Then in table of features is good to tick all common HTTP features, in Application Development CGI in case of further using PHP, HTTP Logging, Logging tools and Request monitor in Health and Diagnostics, All fields in security if not preferable, the request filtering and IP and Domain Restrictions are recommended. For last IIS Management Console is also usable for us as the console is going to be implemented in Server Manager.
- Note: definition of each feature is shortly listed in right top corner. Link to detailed help is also included.



Web Server
- Common HTTP Features
  - Static Content
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - HTTP Redirection
- Application Development
  - CGI
- Health and Diagnostics
  - HTTP Logging
  - Logging Tools
  - Request Monitor
- Security
  - Request Filtering
  - IP and Domain Restrictions
- Performance
  - Static Content Compression

Management Tools
- IIS Management Console

Figure 16 – List of installed features to be accepted before installation.

- After clicking next and checking again the list of features we press install.
- Restart the machine.

Configuration

The configuration is also made in server manager under roles – web server (IIS). On the right part of view is possible to show all the features that are to configure.

- Clicking Default Web Site is possible to show all possible configurations.
- Managing default document is possible to rename the document as index.html located in site root folder.
- Right click the Default Web Site and Explore show the site root folder where the files are located.
- Editting the bindings is important for https connections as shown later.
- IPv4 address and Domain Restrictions is the part of access settings for scopes of users.
- IIS also corresponds with DNS service as each website can be set with the same IP address but other domain name. It also need to be set-up in DNS server as a record.

12.7 Secure Socket Layer - SSL

As examined before Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security for communication over networks. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end. In our case, we use now SSL protocol to create secured HTTP connection using HTTPS protocol. This protocol is secured by encryption using SSL certificate. These certificates contain public and private keys and hash code for identification. In our lab situation, we use self-signed certificate that only allows the SSL protocol works. Private and public key will be created, but in really secured applications, it is important to ask the certification authority. Assigning trusted certificate that is to check at the certification authority for web server[14], which is automatically connected through the client web browser. Browser will ban our certificate as this is self-signed certificate and there is no authority for managing the certificate. The certificate is by then very easily corrupted as there might not be any rules to keep the private key secured or it could be corrupted wittingly. Here is possibility to assign the certificate from free certification

[14] Certification authorities are VeriSign, DigiCert, SwissSign, GlobalSign or GeoTrust. For comparing list of authorities se webpage of SSLshoper.com [19]

authority, but the level of security is the same. The browser ban this certificate as there is no trust of the information inputted to the certification server, as it is possible to do online without identity checking.

To create self-signed certificate we may follow steps below:

- Click the rules - the Web Server (IIS) in server manager.
- In right side window we click the web server icon and then Server Certificates.
- In very right column we can click create self signed certificate.
- After editing name, pressing enter we have assigned our certificate, which should be listed in list of certificates.
- Please note that each certificate has expiration date that vary in level of security.

To assign certificate from authority (we get the same level of security [untrusted], but the process is made through the online certification server and simulates the process of assigning the trusted certificate from authority) we might follow steps below:

- Firstly we need to join CAcert account
- Then we need to generate a Certificate Signing Request
- We then need to add the domain we have control of to our account
- System will send an email with a link in it, we open the link in a webbrowser.
- Then we need to submit the contents from the CSR file to CAcert
- CAcert then sends an email with a signed copy of our certificate

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure (website security testing) identification of the server using the certificate. HTTPS is visible on the very left side of address we connect. To configure website to be secured and the communication is encrypted using encryption algorithms we should follow steps below:

- click on the site name in server manager – roles – web server (IIS) – name of web server – sites – name of our website or default web site
- click edit bindings

- edit the only one binding by selecting HTTPS protocol, leaving the port number assigned (443)
- For the SSL certificate we use the certificate we have created using one of two previous manuals.
- After pressing finish we can try by preesing browse web site (https://domain name:443)
- By creating one of the two certificates listed above the web browser appear to ban the site as it is not trusted even though it is secured. This happens because of using the untrusted certification server. For avoiding this behaviour use trusted server in asking for domain certificate. *Rewiev of certification authorities [19]*.

12.8 Mail Services – SMTP/POP3

Simple Mail Transfer Protocol (SMTP) is the basis of Internet e-mail. Its objective is to transfer mail reliably and efficiently. The use for company is obvious so we will spend the most of the time understanding technical view. Technically the service is host-server based. To be more precise there is need for using more than one server. To increase comprehension, definitions of some abbreviations used when explaining the SMTP and POP3 mailing process, the function is described below.

- **MUA –** Mail User Agent refer to any agent acting as a mail client toward an email server, regardless of it being a mail user agent, a relaying server, or a human typing on a terminal. In addition, a web application providing message management, composition, and reception functionality is sometimes considered an email client.
- **MTA –** Mail Transfer Agent is the computer program acting as server application retrieving the email from Mail User Agent and sending it to appropriate server in network that is reliable of email system of destination part, which is known as MDA (discussed in below).
- **MDA –** Mail Delivery Agent is on the same scope of functions but for our exemplary vector of sent data is now acting as MDA. MDA receives mail and store it in its own database waiting for mail request of destination MUA.

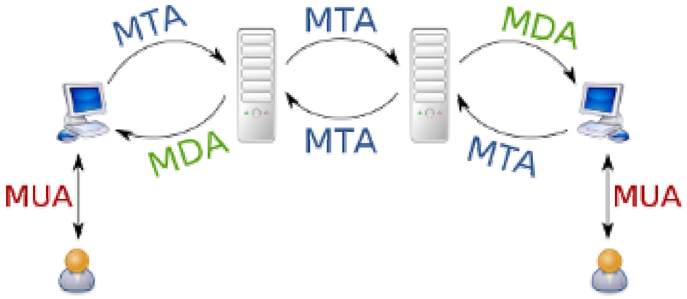


Figure 17 – process model of mail transfer. Source: Wikipedia [20].

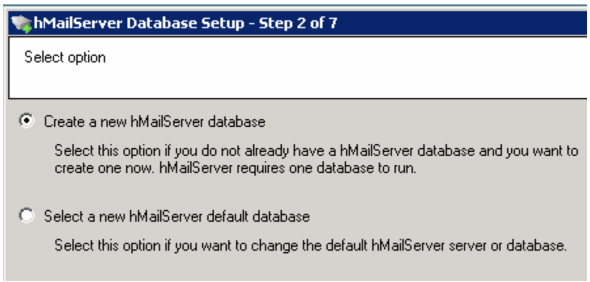
The email process in the above figure – there is mail generated in MUA, then send using SMTP to the MTA. MTA sends it into MDA and after MUA’s request the MDA send the email to destination MUA. Generally, SMTP is the service, which only forwards the mails. For downloading the mail from the server to the destination host POP3, IMAP or HTTP protocol can be used.

MTA/MDA server

Deciding which application to use for covering the MTA/MDA functions is in variety of functions it offers, price and compatibility with the operational system running on the server. We have decided to install HMailServer that covers both the SMTP and POP3 server together, has the administration GUI for settings and administration of accounts. It connects the MySQL database for saving the mails, settings, user profiles and passwords, in order to verify the data created in our database and to select from the selected databases.

Installation

At the installation, the program appears to be configured during, to be able to save the settings for further configuration. First, we can input whether we wish to create a new database or to use an existing database used in past.



hMailServer Database Setup - Step 2 of 7

Select option

● Create a new hMailServer database

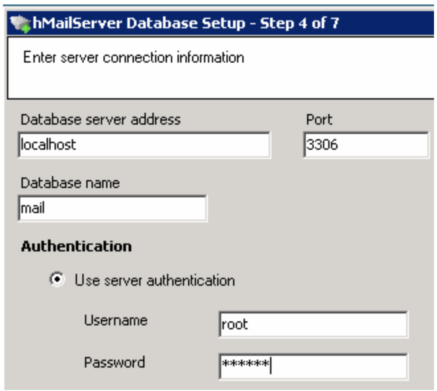
Select this option if you do not already have a hMailServer database and you want to create one now. hMailServer requires one database to run.

○ Select a new hMailServer default database

Select this option if you want to change the default hMailServer server or database.

Figure 18 – Select prompt for a new or an existing database

Once we have decided to create new database, we have chosen the MySQL connection. For typing the database server address on the machine, where runs the database server we can use the localhost address (127.0.0.1 or localhost) for it, otherwise we need to know the IP address of database server for connecting. The port number is standard 3306 for MySQL database.



hMailServer Database Setup - Step 4 of 7

Enter server connection information

Database server address: localhost

Port: 3306

Database name: mail

Authentication

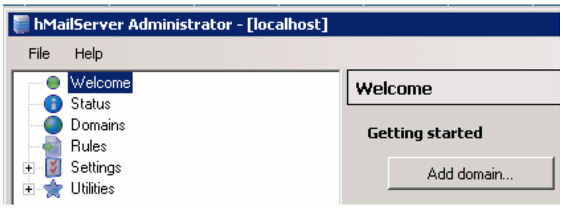
● Use server authentication

Username: root

Password: ******

Figure 19 – Settings for MySQL connection.

Configuration



hMailServer Administrator - [localhost]

Figure 20 – Welcome screen in HMailServer

The configuration is made in following steps:

- Configure DNS records

  ```
  mail.sema.fai.utb.cz        A      195.178.89.12
  sema.fai.utb.cz             MX     [20] mail.sema.utb.cz
  ```

  Note: We have not created more mail servers (as we should as well as with DNS servers) and that is why the DNS records table look simple. The complicating factor is creating more servers and directing the mail traffic into more servers with different IP addresses even with spread in specific ratio.

- Launch hMail server configuration GUI.
- Connect to administration GUI (insert administrator login details).
- Configuring the domain we have rights to (sema.fai.utb.cz).
- Save the settings
- On the domain expanding tree we add all the account addressess
- Assigning the public SMTP host name we go toSettings -> Protocols -> SMTP -> Delivery of e-mail and input sema.fai.utb.cz
- Save the change

After this process the SMTP and POP3 server runs.

Common attack – POP3 Spoofing

As mentioned previously, the spoofing is a very common technique for hackers. Email spoofing is one of these. An unencrypted mail message contains the sent password as standard text. If some equipment listens to the network data flow, it is easy to determine the password. For details, please consult section 7.2 and Code 1.

Prevention

Prevention is in using the secured services for mailing SSL in a POP3 communication between the server and user by downloading the mail using the password for authentication for the account. For details, consult section 12.7.

DISCUSSION

The most important element of the research discussed in this thesis is the focus on security threats that may occur in an operative and functional network. It is also focuses on the importance of the connotation of the significances between all services. It is very important to fully comprehend the services, but equally crucial to understand the meanings that join them together. An additional benefit of this argument is the structured information displayed in bullets or table format. In the case of the network, it is a ready-made solution described step-by step to facilitate configuration.

The thesis fully supports the fundamentals described at the start of the paper.

- Description of the operational system;
- Installation and configuration of the operational systems and network services; configuration
- Research for network security threats and risks;
- Solutions and precautions to avoid security threats.

Part of the deveopment of the thesis is to comment more on security threats as they develop over time.. It is also then possible to provide supplementary details from the networking essetials, operational systems or IT to establish a manual for a wide audience who are interested in this field of expertise. It could also include more case studies using varying networks and their particular requirements. Lastly, consultation and research were an integral part of the development of this academic work often in the form of study reference manual including some validation, quizes, excercises, example studies of error solutions, etc.

CONCLUSION

The benefits of this diploma thesis to the industry and its practitioners are in the provisioning of essential information regarding the enterprise network with the focus on security threats that may occur. A continuous approach to the details in security derives from the basic essentials. Even new network designers and administrators seeking advice do not need to read through the entire paper. It is possible to find the information about service implementation and configuration, while obtaining the logic behind the exact applied security solution.

At the centre of this discussion lie the benefits in obtaining very specific information relative to operating system architecture and other irrelevant information that only take time while studying. The paper will be published as a series of online articles. In doing so, this enables me to study the readers' needs and to focus more on the business aspects of the theory. This entire process has prompted a number of ideas while offering personal satisfaction and self-fulfilment.

LIST OF LITERATURE

[1] STANEK, William R. *Microsoft Windows Server 2008 : kapesní rádce administrátora*. Brno : Computer Press, 2008. 704 s. ISBN 978-80-251-1936-5.

[2] LUDVÍK, Miroslav, ŠTĚDROŇ, Bohumír. *Teorie bezpečnosti počítačových sítí*. Kralice na Hané : Computer Media, 2008. 98 s. ISBN 978-80-86686-35-6.

[3] MCCLURE, Stuart, SCAMBRAY, Joel, KURTZ, George. *Hacking bez záhad*. Praha : Grada, 2007. 520 s. ISBN 978-80-247-1502-5.

[4] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Brno : CP Books, 2005. 338 s. ISBN 80-251-0417-6.

[5] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí : praktické rady a návody*. Praha : Grada, 2003. 200 s. ISBN 8024706636.

[6] HORÁK, Jaroslav, KERŠLÁGER, Milan. *Počítačové sítě pro začínající správce*. 4. rozš. vyd. Brno : Computer Press, 2008. 327 s. ISBN 978-80-251-2073-6.

[7] KABELOVÁ, Alena, DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5. aktualiz. vyd. Brno : Computer Press, 2008. 488 s. ISBN 978-80-251-2236-5.

[8] TRULOVE, James. *Sítě LAN: hardware, instalace a zapojení*. 1. vyd. Praha : Grada, 2009. 384 s. ISBN 978-80-247-2098-2.

[9] ENDORF, Carl, SCHULTZ, Eugene, MELLANDER, Jim. *Detekce a prevence počítačového útoku*. 1. vyd. Praha : Grada, 2005. 355 s. ISBN 8024710358.

[10] BIGELOW, Stephen J. *Mistrovství v počítačových sítích : správa, konfigurace, diagnostika a řešení problémů*. 1. vyd. Brno : Computer Press, 2004. 990 s. ISBN 8025101789.

[11] FARNSWORTH, William. The SANS™ Institute [online]. 2010 [cit. 2010-03-20]. *Information Security Policy - A Development Guide for Large and Small Companies*. Available from WWW: <http://www.sans.org/reading_room/whitepapers/policyissues/information_security_policy_a_development_guide_for_large_and_small_companies_1331>.

[12] *Microsoft Technet : Windows 2008 Server* [online]. 2010 [cit. 2010-03-20]. Common Types of Network Attacks. Available from WWW: <http://technet.microsoft.com/en-us/library/cc959354.aspx>.

[13] *Hacker (computer security) In Wikipedia: the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, , [cit. 2010-03-20]. Available from WWW: <http://en.wikipedia.org/wiki/Hacker_(computer_security)>.

[14] *IBM Support* [online]. 2010 [cit. 2010-03-20]. How SSL Works. Available from WWW: <http://publib.boulder.ibm.com/tividd/td/TRM/GC32-1323-00/en_US/HTML/admin231.htm#idx718>.

[15] Cisco Systems, Inc. *Cisco.com: Internetworking Technology Handbook* [online]. 2009 [cit. 2010-03-24]. Available from WWW: <http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Routing-Basics.html>

[16] *List of DNS record types* In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, , [cit. 2010-03-29]. Available from WWW: <http://en.wikipedia.org/wiki/List_of_DNS_record_types>

[17] *Firewall (computing) In Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, , [cit. 2010-04-05]. Available from WWW: <http://en.wikipedia.org/wiki/Firewall_(computing)>.

[18] *Netcraft* [online]. 2010 [cit. 2010-04-08]. January 2010 Web Server Survey. Available from WWW: <http://news.netcraft.com/archives/2010/01/>.

[19] *SSL Shopper* [online]. 2010 [cit. 2010-04-09]. SSL Certificate Reviews. Available from WWW: <http://www.sslshopper.com/certificate-authority-reviews.html>.

[20] Picture in *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, , [cit. 2010-04-11]. Available from WWW: <http://commons.wikimedia.org/w/index.php?title=File:MTA-MDA-MUA_relationship.svg&oldid=34606124>.

[21] *Directions on Microsoft* [online]. 2010 [cit. 2010-04-12]. Windows Server 2008 Edition Comparison. Available from WWW: <http://www.directionsonmicrosoft.com/sample/DOMIS/update/2008/02feb/0208ws2plp_ch.htm>.

[22] *US-CERT : Vulnerability Notes Database* [online]. 2008-07-08, 2009-06-03 [cit. 2010-04-16]. Vulnerability Note VU#800113. Available from WWW: <http://www.kb.cert.org/vuls/id/800113>.

[23] LARSON, Robert E.; COCKCROFT, Lance. *CCSP: Cisco Certified Security Professional Certification : All In One - Exam Guide*. New York : McGraw-Hill/Osborne, 2003. 984 s. ISBN 0-07-222691-9.

[24] *Windows Server 2008* [online]. 2010 [cit. 2010-04-19]. Product Information. Available from WWW: <http://www.microsoft.com/windowsserver2008/en/us/product-information.aspx>.

[25] Windows Server 2008 In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, , [cit. 2010-04-19]. Available from WWW: <http://cs.wikipedia.org/wiki/Windows_Server_2008>.

[26] *Connectworld.net* [online]. 2008 [cit. 2010-04-20]. Employee Internet Use. Available from WWW: <http://www.connectworld.net/ccc/employee-internet-usage.html>.

[27] *Snapshotspy.com* [online]. 2008 [cit. 2010-04-20]. Employee Computer & Internet Abuse Statistics. Available from WWW: <http://www.snapshotspy.com/employee-computer-abuse-statistics.htm>.

[28] *Youtube.com* [online]. 2008 [cit. 2010-05-29]. *The IT Crowd - What Does IT Stand for?* . Available from WWW: <http://youtube.com/watch?v=LUA9oNCubgk>.

LIST OF SYMBOLS, ACRONYMS AND ABBREVIATIONS

AD	Active Directory
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ASLR	Address space layout randomization
ASP	Active Server Pages
AUX	Auxiliary port
CPU	Central Processing Unit
CSMA/CD	Carrier Sense Multiple Access
DES	Data Encryption Standard
DNS	Domain Name System
DNSSEC	Domain Name System Security
DVD	Digital Video Disc
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMS	Electromagnetic Susceptibility
FTP	File Transfer Protocol
GUI	Graphic User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IIS	Internet Information Services
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet service provider
IT	Information Technology [28]
LAN	Local Area Network
MAC	Media Access Control address
MAN	Metropolitan Area Network
MDA	Mail Delivery Agent
MS	Microsoft
MTA	Mail Transfer Agent
MUA	Mail User Agent

MySQL	Relational Database Management System (product of SUN)
NAT	Network Access Translation
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
OSI	Open Systems Interconnection
PC	Personal Computer
PHP	Hypertext Preprocessor
POP3	Post Office Protocol
RAM	Random access memory
RRAS	Routing and Remote Access Services
RSA	Rivest, Shamir and Adleman (an algorithm for public-key encryption)
SCP	Session Control Protocol
SQL	Structure Querry Language
SSH	Secure Shell Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WAN	Wide area network
WDS	Windows Deployment Services
WEB	World Wide Web
WFAS	Windows Firewall with Advanced Security
WMI	Windows Management Instrumentation
ZIP	Zone Information Protocol

LIST OF FIGURES

Figure 1 - Schema of standard switch interconnection.. 44

Figure 2 - Wiring of each standard 45

Figure 3 - Wiring of each standard 45

Figure 4 – Physical schema of the network 47

Figure 5 – IP model of the network 48

Figure 6 – settings of routing in server manager.. 50

Figure 7 – sample diagram of DNS hierarchy 54

Figure 8 – list of possible DNS records as a right click to particular forward lookup zone 56

Figure 9 – The DNS records in our server.. 57

Figure 10 – selecting the role of DHCP server for installing................................. 59

Figure 11 – adding domain and DNS server... 59

Figure 12 – DHCP scope configuration.. 60

Figure 13 –network rules configuration in windows firewall - server manager. 62

Figure 14 – types of rules.. 62

Figure 15 – settings for the rule after double-click... 63

Figure 16 – List of installed features to be accepted before installation.............................. 66

Figure 17 – process model of mail transfer. Source: Wikipedia [20]. 70

Figure 18 – Select prompt for a new or an existing database 71

Figure 19 – Settings for MySQL connection. 71

Figure 20 – Welcome screen in HMailServer... 71

LIST OF TABLES

Table 1 – Comparison of distributions of MS Windows Server 2008, Source [21]. 12

Table 2 – Sample security policy, Source: William Farnsworth, Sans Institute [1] 16

Table 3 – List of commonly used protocols over SSL/TLS... 26

Table 4 – list of web servers in order of usage. Source: Netcraft [18]. 65

ATTACHMENT I – SECURITY STATISTICS

General Internet Misuse

One-third of time spent online at work is non-work-related. Internet misuse at work is costing American corporations more than $85 billion annually in lost productivity. Eighty percent (80%) of companies reported that employees had abused Internet privileges, such as downloading pornography or pirated software.

Employee Hacking

Sevety-five (75%) of companies cited employees as a likely source of hacking attacks. 45% of businesses had reported unauthorized access by insiders.

Instant Messaging

Nearly eighty percent (80%) of instant messaging in companies is done over public IM services such as AOL, MSN and Yahoo, exposing companies to security risks. There are more than 43 million users of consumer IM at work. Only one quarter of companies, have a clearly defined policy on the user of IM at work.

P2P File Sharing

Forty-five (45%) percent of the executable files downloaded through Kazaa contain malicious code. 73 percent of all movie searches on file-sharing networks were for pornography. A company can be liable for up to $150K per pirated work if it is allowing employees to use the corporate network to download copyrighted material.

Adult / Porn Sites

70 percent of porn is downloaded between 9am and 5pm. 37 percent of at-work Internet users in the US had visited an X-rated Web site from work.

Spyware

1 in 3 companies have detected spyware on their network. There exist more than 7,000 spyware programs.

Streaming Media

77 percent of weekly online listening to Internet Radio takes place between 5 a.m. and 5 p.m. Pacific time. 44 percent of corporate employees actively use streaming media.

Computer Viruses / Malicious Code

Although 99% of companies use antivirus software, viruses and worms hit 82% of them. Blended threats made up 54 percent of the top 10 malicious code submissions over the last six months of 2003. The number of malicious code attacks with backdoors, which are often used to steal confidential data, rose nearly 50% in the last year.

Source: Connectworld [26].

- 30 to 40% of Internet use in the workplace is not related to business.
- 64% of employees say they use the Internet for personal interest during working hours.
- 70% of all Internet porn traffic occurs during the nine-to-five work day.
- 37% of workers say they surf the Web constantly at work.
- 77.7% of major U.S. companies keep tabs on employees by checking their e-mail, Internet, phone calls, computer files, or by videotaping them at work.
- 63% of companies monitor workers' Internet connections and 47% store and review employee e-mail.
- 27% of companies say that they've fired employees for misuse of office e-mail or Internet connections, and 65% report some disciplinary measure for those offenses.
- According to a survey by International Data Corp (IDC), 30 to 40% of internet access is spent on non work related browsing, and a staggering 60% of all online purchases are made during working hours.
- 90 percent of employees feel the Internet can be addictive, and 41 percent admit to personal surfing at work for more than three hours per week.
- Some estimates reveal that computer crime may cost as much as $50 billion per year.
- Around 80% of computer crime is committed by "insiders". They manage to steal $100 million by some estimates; $1 billion by others.
- The average fraud inflicts a loss of about $110,000 per corporate/organization victim, and $15,000 to each individual victim.
- 60% of Security Breaches occur within the Company - behind the Firewall
- 25% of corporate Internet traffic is considered to be "unrelated to work".
- 30-40% of lost productivity is accounted for by cyber-slacking.
- Most studies show 70% of companies have had sex sites accessed using their network.
- 32.6% of workers surf the net with no specific objective; men are twice as likely as women.

- When asked "should employers monitor, limit, block or control the Internet access while at work?" over 60 % of employees said "yes".
- On average, workers spend 21 hours per week online at the office, as oppose to only 9.5 hours at home
- 27% of Fortune 500 organisations have defended themselves against claims of sexual harassment stemming from inappropriate email.
- Traditionally, employers have been responsible and liable for the actions of their employees in the workplace. However, if an organisation can demonstrate a "duty of care" to reduce unacceptable employee activity, then it could minimize it's potential for liability.
- Chevron faces a $2 million lawsuit as a result of an employee's email that allegedly included sexist content.
- A company with 1,000 Internet users could lose upwards of $35 million in productivity annually from an hour of daily Web surfing by employees
- 90% of respondents (primarily large corporations and government agencies) detected computer security breaches within the previous 12 months, 80% acknowledged financial losses due to computer breaches, 44% were willing and/or able to quantify their losses, at more than $455 million.
- The most serious financial losses occurred through theft of proprietary information respondents reported more than $170 million) and financial fraud (respondents reported approximately $116 million).
- Estimated that the greatest threat to intellectual property is trusted insiders; 70% of security breaches come from inside.

Source: Snapshotspy [27].