SECURITY OF DISTRIBUTED SYSTEMS

E. A. Basynya, D. S. Khudiakov

NOVOSIBIRSK
2020
Ph.D in Technical Science, prof. of the Automation Department in NSTU, Director of the Institute of Information and Communication Technology **E.A. Basynya**

Ph.D in Technical Science, prof. of the Automation Department in NSTU **D.S. Khudiakov**


Reviewers:

Doctor of Technical Science, prof. of the Automation Department in NSTU G.A. Frantsuzova,

Doctor of Technical Science, prof. of the Data acquisition and processing systems Department in NSTU V.I. Guzhov

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The book is intended for students enrolled in the program “Technology of Internet of Things and Smart City”. The book includes training materials and guidelines for self-monitoring (questions for self-testing). For successful study of the course, the diligent training in previously studied IT disciplines is required.
Contents

DEFINITIONS AND ABBREVIATIONS .............................................................................................. 6
INTRODUCTION .......................................................................................................................... 9

1. DISTRIBUTED CORPORATE COMPUTER NETWORK DESIGN, COMPLEX FIREWALL INTEGRATION .............................................................................................................................. 10
   1.1. Design of CCN ...................................................................................................................... 10
       1.1.1 Managed Network Equipment Functions ........................................................................ 10
       1.1.2. Design tool .................................................................................................................... 12
       1.1.3. Practical guidelines ....................................................................................................... 12
   1.2. Server OS installation and configuration ........................................................................... 13
   1.3. Firewall Configuration ....................................................................................................... 13
   1.4. Remote network access implementation ............................................................................. 15
   1.5. Practical task ....................................................................................................................... 15
   1.6. Control questions ................................................................................................................ 16

2. DISTRIBUTED WEB SYSTEMS AND WEB APPLICATION LAYER FIREWALLS ............ 17
   2.1. Web servers ........................................................................................................................ 17
   2.2. The main security threats to web resources ....................................................................... 17
   2.3. Practical task ....................................................................................................................... 19
   2.4. Control questions ................................................................................................................ 19

3. FILE SERVERS .......................................................................................................................... 20
   3.1. Centralized file sharing technologies ................................................................................... 20
   3.2. Decentralized File Sharing Technologies ............................................................................ 21
   3.3. Practical task ....................................................................................................................... 22
   3.4. Control questions ................................................................................................................ 22

4. BASICS OF ADMINISTRATION OF CENTRALIZED WORK OF USERS IN DISTRIBUTED SYSTEMS .......................................................................................................................... 23
   4.1. Terminal server .................................................................................................................... 23
   4.2. Application virtualization ................................................................................................... 24
   4.3. Active Directory .................................................................................................................. 24
   4.4. Practical task ....................................................................................................................... 26
   4.5. Control questions ................................................................................................................ 27

5. AUDIT OF INFORMATION SECURITY OF DISTRIBUTED COMPUTER NETWORKS AND INFORMATION SYSTEMS ........................................................................................................... 28
   5.1. Theoretical bases of vulnerability analysis of information systems and computer networks 28
11.2. Design and implementation of the system ................................................................. 53
11.3. The discussion of the results ..................................................................................... 58
11.4. Practical task ........................................................................................................... 58
11.5. Control questions..................................................................................................... 59
CONCLUSION .................................................................................................................. 60
REFERENCES .................................................................................................................. 61
Definitions and Abbreviations

ACL — Access Control List
AD — Active Directory
AES — Advanced Encryption Standard
ARP — Address Resolution Protocol
BIOS — Basic input/output system
BT — BitTorrent
CAPTCHA — Completely Automated Public Turing test to tell Computers and Humans Apart
CCN — Corporate Computer Network
CIPF — Cryptographic Information Protection Facilities
CIPF — Cryptographic Information Protection Facility
CSRF — Cross Site Request Forgery
DB — Database
DBMS — Database Management System
DDoS attack — Distributed Denial of Service attack
DHCP — Dynamic Host Configuration Protocol
DLP — Data loss prevention
DMZ — Demilitarized Zone
DNAT — Destination Network Address Translation
DNS — Domain Name System
DS — Digital signature
EDS — Electronic digital signature
EIA — Electronic Industries Association
FDDI — Fiber Distributed Data Interface
FTP — File Transfer Protocol
FTPS — File Transfer Protocol + SSL, FTP/SSL
FW — Firewall
GUI — Graphical User Interface
HIDS/HIPS — Host-based IDS/IPS
HTML — HyperText Markup Language
HTTP — HyperText Transfer Protocol
HTTPS — HyperText Transfer Protocol Secure
I2P — Invisible Internet Project
ICMP — Internet Control Message Protocol
ICT — Information and Communications Technology
IDS — Intrusion Detection System
IPS — Intrusion Prevention System
IPSec — IP Security
IS — Information Security
ITSM — IT Service Management
JAP — Java Anonymous Proxy
JTR — John The Ripper
KVM — Kernel-based Virtual Machine
L2 — a data link layer device of the OSI model
L2+ — a data link layer device of the OSI model, partially including the functionality of the overlying layers
L2P — Layer 2 Tunnel Protocol
L2TP — Layer 2 Tunneling Protocol
LAN — Local Area Network
LVM — Logical Volume Manager
MIB — Management Information Base
MLC — Multi-Level Cell
MS-CHAP — Microsoft version of the Challenge-Handshake Authentication Protocol
NAS — Network Attached Storage
NAT — Network Address Translation
NGFW — Next Generation Firewall
NGFW — Next-generation firewall
NIDS/NIPS — Network-based IDS/IPS
NMS — Network Management Stations
NTFS — New Technology File System
OS — Operating system
OSI — Open Systems Interconnection basic reference model
OTR — Off-the-Record
p2p — peer-to-peer
PAP — Password Authentication Protocol
PCoIP — PC-over-IP
PDF — Portable Document Format
PGP — Pretty Good Privacy
PoE — Power over Ethernet
PPTP — Point-to-Point Tunneling Protocol
RAID — Redundant Array of Independent Disks
RDP — Remote Desktop Protocol
S/MIME — Secure/Multipurpose Internet Mail Extensions
S/W — Software
SAN — Storage Area Network
SAS — Serial Attached SCSI
SATA — Serial Advanced Technology Attachment
SFTP — SSH File Transfer Protocol
SIEM — Security information and event management
SLA — Service Level Agreement
SNAT — Source Network Address Translation
SNMP — Simple Network Management Protocol
SOCKS — SOCKet Secure
SQL — Structured Query Language
SSD — Solid-state drive
SSH — Secure Shell
SSL — Secure Sockets Layer
STP — Spanning Tree Protocol
Syslog — System log
Tails — The Amnesic Incognito Live System
TCP/IP — Transmission Control Protocol/Internet Protocol
TELNET — TElminal NETwork
TIA — Telecommunications Industries Association
TLC — Triple-Level Cell
TLS — Transport Layer Security
TOR — The Onion Router
UML — Unified Modeling Language
URL — Uniform Resource Locator
USB — Universal Serial Bus
UTM — Unified threat management
UTM — Urchin Tracking Module
UTP — Unshielded Twisted Pair
vCLI — vSphere Command Line Interface
VDI — Virtual Desktop Infrastructure
VE — Virtual Environments
VLAN — Virtual Local Area Network
VM — Virtual machine
VPN — Virtual Private Network
VSC — Virtualization Service Client
VSP — Virtualization Service Provider
WebDAV — Web Distributed Authoring and Versioning
XML — Extensible Markup Language
XMPP — Extensible Messaging and Presence Protocol
XSS — Cross-Site Scripting
Introduction

Information and communication technology have acquired a global transboundary nature and have become an integral part of all areas of activity of the state, society and the individual. Private companies and government agencies organize packet-switched local area networks based on the TCP/IP protocol stack. Vulnerabilities of this stack, operating systems, defenses, software, algorithms, methods and protocols can be used by attackers to do significant economic, social or political damage. Accordingly, information security issues have become increasingly strategic.

This tutorial is the result of the fruitful and efficient work of the Novosibirsk State Technical University under the program "SMARTCITY: Innovative Approach Towards a Master Program on Smart Cities Technologies" (which lasted from 15 November 2018 to 14 November 2021). Its goal is to create a new generation of interdisciplinary engineers of information and communication technologies in the field of Smart Cities. The project complies with the principles of the Bologna process and aims to develop the European Higher Education Area. The purpose of the publication is the formation of professional skills and competencies of future specialists in the field of system administration, an integral part of which is the theory of computer systems and networks with the security of distributed information resources. It is worth noting that a conceptual understanding of the material presented is the basis of any profession in the field of information technology. Readers are required to develop skills for searching, processing, systematizing and analyzing of information. It is necessary to learn how to make informed, constructive and reasoned decisions, study the material at a conceptual level and quickly solve the tasks in the shortest possible time.
Keywords: port security, IP-binding, ACL, VLAN, SNMP, Trunk, STP, VirtualBox, LVM, RAID, Windows, Unix/Linux, Ansible, Docker, Kubernetes NAT, DMZ, Kerio control, Traffic inspector, iptables, FirewallD, SELinux, RDP, SSH, SSL, TLS.

This chapter focuses on the basics of designing distributed corporate computer networks. Various options for installing and configuring network equipment, ensuring the performance and fault tolerance of nodes, ensuring network information security and delimiting access to internal and external network resources, and also implementing remote network access are considered.

All practical tasks can be performed both in terminal classes and on your own personal computers at home. It is recommended to use virtualization software programs of operating systems in order to avoid data loss and the negative effects of potential errors. One possible solution is VirtualBox. It is free open source code software and distributed under the terms of the General Public License.

1.1. Design of CCN

It is necessary to set the initial conditions for the reasoned choice of the server operating system, i.e. need to design an area network of the enterprise, which will act as a customer. The number of working hosts is 100 units. When placing network equipment, don't forget to provide key information on its configuration.

For example, controlled switches (L2+) can provide a wide range of information security opportunities. Consider the most well-known Local Area Network (LAN) security mechanisms used in controlled network devices.

1.1.1 Managed Network Equipment Functions

The most common switch functions for information security are:

1) port security — binding of MAC addresses to device ports;
2) IP-binding — binding of MAC addresses to IP addresses;
3) access control implementation (Access Control List);
4) spanning tree protocol configuration (STP);
5) network segmentation into logical sub-networks (VLAN — Virtual Local Area Network);
6) network management SNMP (Simple Network Management Protocol).

Port security is a function of binding MAC addresses to device ports or specifying the number of allowed MAC addresses. If the parameters don't match, traffic is blocked. Using this function of network devices, e.g. switches, allows to prevent unauthorized connection to the network, as well as to exclude the possibility of a series of attacks aimed at overflowing the table of information streams promotion.

IP-binding is a function that fixes the connection of MAC and IP addresses. If there is a mismatch, traffic is rejected by the switch. In modern network devices, manufacturers generally combine this function with port security and call it IP-MAC-Port Binding.
Equally useful is the Spanning Tree Protocol (STP), which disables redundant communication links to prevent loops, and reactivates links in the presence of single points of failure. The technology of port aggregation into a single logical object (trunk) will help to expand communication bandwidth. Bandwidth is added up.

**Access Control List, Virtual Local Area Network** and **SNMP** require more detailed consideration.

**Access Control List (ACL)** is a mechanism for filtering traffic, performed in accordance with specified criteria, represented as a set of text expressions. Access control lists can be used for a variety of purposes: perform packet filtering; restrict access to the router; specify traffic to perform encryption; determine the priority of traffic processing; specify network addresses for translation, etc.

These are two main categories of **ACL**: standard access control lists and extended access control lists. Standard lists provide the ability to filter traffic by a single criterion — the sender's address, while extended ones have a much larger list of parameters: sender and receiver addresses, TCP/UDP ports of sender and receiver, the used transmission control protocol (TCP) and the type of traffic for this protocol (for example, only redirect messages is used to filter for ICMP — Internet Control Message Protocol), etc.

The following technologies can be added to the capabilities of advanced access control lists:

1. **Dynamic ACLs** allow to resolve data transmission through the router for a period of time. After connecting to a network device and authenticating the user, the dynamic list is added to the existing extended list. It is possible to specify the time interval after which the dynamic record is removed from the list if it isn't used;
2. **Reflexive ACLs** allow packet filtering based on information about sessions that occur inside the router: inbound traffic is allowed only if a node has previously accessed the resource;
3. **Time-based ACLs** provide network access on the basis of time period that specifies a particular time of day and/or day of the week. For example, one can allow access to the external network from Monday to Friday during working hours, using these lists.

Both standard and extended access control lists can be set in two ways: numbered and named. It makes more sense to use named lists because one can edit them line by line, while in numbered lists, new rows can be added only at the end.

To configure the **ACL** correctly, it is necessary to remember the following:

1. packets are processed strictly in the order in which conditions are specified;
2. if a packet falls under any condition, it stops processing;
3. each list contains an implicit deny any command at the end;
4. lists should be placed according to the following rules: extended — close to the source, standard — close to the receiver;
5. one can place no more than one list per interface, protocol or direction;
6. access control lists don't affect traffic generated by the router.

A **Virtual Local Area Network (VLAN)** is a mechanism for creating a logical network topology that is independent of its physical topology. **VLAN** operation is based on the **IEEE 802.1Q** standard. Network devices integrated into one logical sub-network communicate directly at the data link layer, regardless of their actual location. In contrast, devices connected to the same switch but located on different logical sub-networks remain invisible to each other at the data link layer.

The use of this technology has a number of advantages:

1. the possibility of flexible dividing network devices into groups: each **VLAN** has its own subnet; devices that are located at a distance from each other can be located on the same subnet regardless. **VLAN** makes it much easier to add new devices or change the connections between them;
2. reducing network load by reducing the amount of broadcast traffic: a single switch can be divided into multiple broadcast domains;
3. preventing broadcast storms on the network;
4. reducing bandwidth consumption (compared to the case of a single broadcast domain);
5. simplification of the ensuring network security task: using **VLAN** policy and security rules, this technology can be applied to the entire subnet, rather than to individual devices.

The purpose of the **SNMP** protocol is to collect information about the situation on the Internet by **Network Management Stations (NMS)**. The data format is set by the protocol, and their processing and
SECURITY OF DISTRIBUTED SYSTEMS

interpretation are determined by the management stations. The protocol is based on the concept that all the necessary information for controlling managed device is stored on the device itself — in the Management Information Base (MIB). The MIB contains a set of variables served by the SNMP agent. They characterize the state of the managed object and describe its various parameters: device interfaces status, number of packets processed by the device, operation time, etc. In addition to the standard variables, each manufacturer can add any device-specific parameters to the controlling database. The MIB is updated by the device itself regularly.

SNMP as a network protocol is something like a set of commands to work with MIB variables. To control the operation of a network device, it is necessary to access its MIB and analyze the values of the corresponding variables. The simplicity of the network management protocol is achieved by the absence of specific commands to control network devices — instead, MIB variables are switched, which is perceived as an indication to execute a command by the node. At the same time, SNMP is a powerful tool that allows to specify command sets for managing network devices in a standardized way. Therefore, command execution is achieved by registering the variables in the MIB and the device's response to their change.

1.1.2. Design tool

At the present time, there are many tools for modelling and designing corporate computer networks on the market. Using such tools allows to make a competent choice of network topology, architecture and concept of information security. It is worth to list the most common of them:

1) Cisco Packet Tracer is a network modelling program that provides a wide range of capabilities. It allows to experiment with network behavior, test topologies for performance, and simulate various scenarios. The packet includes a series of Cisco switches and routers, ASA 5505 firewall, FTP, DNS, Syslog, DHCP servers, etc. This tool helps you gain practical configuration skills for various protocols and network devices with Cisco IOS commands. Cisco Packet Tracer is available free of charge for Cisco Networking Academy students;
2) Microsoft Visio is a tool for creating diagrams and flowcharts for Windows. One can create graphical displays of various tasks using the built-in templates of this tool: management tasks, application development, security system planning, etc;
3) online design tools — draw.io, gliffy.com, creately.com are convenient solutions that don't require installation. They include sets of elements for many diagram types: UML (Unified Modeling Language), connections, flowcharts, tools for creating iOS structures and Android applications, etc.

Almost every network equipment manufacturer offers modelling and design software. Each of these tools has both advantages and disadvantages. The choice of a particular modelling tool depends on the requirements of the network project and your personal preferences.

1.1.3. Practical guidelines

One of the most important network components is the cabling system. Errors made in its design, can cause difficulties in troubleshooting process in the future. When laying a new wiring or performing an update to an existing one, one should adhere to the standards of the Telecommunications Industries Association (TIA) and Electronic Industries Association (EIA). These standards provide for the use of shielded and unshielded twisted pair as well as optical cable.

The most commonly used UTP cable (Unshielded Twisted Pair) provides the most flexibility at the lowest cost. Category 5 cables are recommended for local area networks because they support high-speed protocols. Most high-speed technologies (Fast Ethernet, Gigabit Ethernet, FDDI, etc.) are focused on the use of this cable category.

Installation of a fiber optic system is more expensive due to the higher cost of network equipment designed for this connection type. However, fiber optic cable has significant advantages over twisted pair: higher data rates and the ability to transmit data over long distances. Another important aspect is the immunity to electromagnetic interference. That is why it is recommended to choose fiber optic cable when it is necessary to do outdoor cable installation.
When a cable system is being designed, it is necessary to provide for the possibility of its expansion regardless of selected medium type chosen — to increase the channels diameter for laying the cable in advance. This will make it easy to run an additional cable, both UTP and optical.

When choosing network equipment, namely switches, it is necessary to take into account the implemented method of packet transmission and buffering, as well as the availability of support for PoE technology (Power over Ethernet). This technology is described by the IEEE 802.3 af-2003 and IEEE 802.3 at-2009 standards, and allows the Ethernet switch to transmit electric power to end devices (IP camera, Wi-Fi module, etc.) through a standard twisted pair. PoE-enabled switches have a higher cost; however, their implementation avoids additional cabling to each device.

1.2. Server OS installation and configuration

Deploying any server solution, it is always necessary to predict the prospects for further development of the company, respectively, and further requirements for the host. First of all, there is the question of performance and fault tolerance. To solve this problem will help a competent choice of equipment and set up an array of several storage devices managed by a controller, connected to each other by high-speed communication channels and perceived by the external system as a whole. The technology is called a RAID (Redundant Array of Independent Disks). The controller can be represented by both hardware and software implementation. A different degree of fault tolerance and performance (read speed or write data) is provided depending on the type of array used. For example, RAID 0 is a high-performance disk array with striping and no fault tolerance, and RAID 1 is a mirror disk array with fault tolerance. It is usually referred to as Mirroring.

Imagine the situation: a file server was configured on Linux, but disk space exhausted quickly. One should insert additional storage device and reconfigure the server to work correctly with the data over the network. In order to save time, it is possible to pre-connect the disk space management technology that operates on top of the logical partitions at the system installation (Logical Volume Manager, LVM). This will allow for more flexible use of disk space. The main scope of LVM — file storage, databases. By configuring this tool, you combine physical data storage devices into single virtual logical unit, i.e. you create single virtual disk of total volume. Then you randomly divide its space. The /boot partition cannot be located in a logical volume group because the boot loader will not be able to read it. When the free space is over, you will need to insert an additional storage device and mount it to the LVM. No additional settings are required. Disk Space Management for Windows has similar (but limited) functionality.

After successful OS installation it is necessary to deal with information security issues, first of all, there is firewall. Among the open source solutions, the optimal one is the iptables packet filter, which is part of the Netfilter firewall built into the Linux kernel and performs traffic filtering and packet forwarding in accordance with specified rules. It is worth noting that in recent versions of Linux, CentOS and RedHat to replace Netfilter (including iptables) came firewalld. However, the refusal to use firewalld does not adversely affect the security of the LAN, since the functionality and capabilities of iptables allow to implement filtering of inbound, outbound and transit traffic at least qualitatively. Before setting it up, it is recommended to carefully read the manual called Iptables Tutorial. An example of configuring a packet filter with the Linux/Unix connection tracer will help you gain a conceptual understanding of the material. Then, you have to conduct a benchmark analysis of possible implementations of the internet gateway and compatible defenses [1-16].

1.3. Firewall Configuration

Consider the technology for performing network address translation — NAT. Note that only the first packet from the stream passes through the chains of the table, address translation or masking is applied to all subsequent packets in the stream automatically. The DNAT (Destination Network Address Translation) action translates destination addresses into packet headers. In other words, this action redirects packets to addresses other than those specified in the packet headers. SNAT (Source Network Address Translation) is used to change the source addresses of packets. You can hide the structure of the local network with this procedure, and at the same time share a single external IP address between computers on
the local network to access the Internet. In this case, the firewall automatically performs forward and reverse address translation using SNAT, thereby making it possible to connect to servers on the Internet from computers on the local network.

Consider an example of configuring the `iptables` packet filter. There are two approaches to its implementation: the default action is to block traffic unless it matches any rule, or allow all actions that are not blocked by any rule. In this example, the first principle is used:

```bash
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
```

Then, a new chain of "bad_tcp_packets" rules is created to handle TCP packets with invalid headers:

```bash
iptables -N bad_tcp_packets
iptables -A bad_tcp_packets -p tcp --tcp-flags SYN,ACK SYN,ACK -m state --state NEW -j REJECT --reject-with tcp-reset
iptables -A bad_tcp_packets -p tcp ! --syn -m state --state NEW -j LOG --log-prefix "New not syn:"
```

A Demilitarized Zone (DMZ) can be used to delimit access to external and internal network resources. It can be configured either by using the built-in functions of the network equipment or by using DNAT technology (Fig. 1):

![Fig. 1. DMZ configuration](image)

Creating a demilitarized zone to minimize damage in the event of an attack on any of the public services: an attacker will not have direct access to the internal network segment.
1.4. Remote network access implementation

Organizing remote access to the information system, don't forget to do filtering by IP-addresses. In addition, it is unacceptable to use the TELNET (TERminal NETwork), SSH (Secure Shell) and RDP (Remote Desktop Protocol) protocols in the standard form. For example, in the last one, you should use TLS (Transport Layer Security), limit the number of incorrect password attempts, enable parameter checking and authentication at the network layer, increase the level of encryption and ACL, etc. In practical terms, the using of these protocols inside secure channel is more substantive and secure decision. For example, to use encapsulation of information streams in VPN (Virtual Private Network). The most well-known implementations of these technologies are IPSec (IP Security), usually used with the protocol L2P (Layer 2 Tunnel Protocol) to ensure the data transmitted security, and OpenVPN. These protocols are discussed in more detail in Chapter 9: "Anonymization on the Internet". Also, don't forget about the Port Knocking technology, which is a scheme of authentication and authorization through a specified sequence of connection attempts to the server ports. The target port is opened after a series of predefined "knocks" recorded on the server side. This way is vulnerable if there is traffic interception by an attacker, therefore, it provides a mechanism for using one-time sequences.

After the corporate computer network project implementation and the virtual implementation of the configured server in the head office, you should analyze the possible consequences and processes during the following types of attacks:

1) fake Address Resolution Protocol (ARP) replies. Falsified ARP messages are sent such that each of the attacked hosts interprets the attacker's MAC address with the address of its interlocutor;
2) imposing a fake router. The imposition of fake routes is performed using falsified Redirect ICMP messages. The attacker's address becomes known as the router's address;
3) forgery during host configuration. It is possible that there's the imposition a fake edge node through a Router Advertisement ICMP message. Alternatively, it could be done through the Dynamic Host Configuration Protocol (DHCP) by issuing the first DHCP offer by a fake server;
4) impact on routing protocols. Falsified routing protocol messages with more favourable parameters are sent to switch the required routes to your own network node. For example, if there are fewer hops (transit nodes);
5) impersonation (it is when someone pretends to be another object) without feedback. This is achieved by changing the content of datagram headers;
6) desynchronize of the TCP connection. It is carried out by sending falsified control messages. The attack tunnelling and bypass filter rules could be fall into this category. For example, using double packet encapsulation;
7) impersonation in order to establish full control over the connection which is called TCP hijacking;
8) using protocols of the application vulnerabilities.

Analytical components on these issues will help to more carefully approach the ensuring of network information security. It should be noted what types of attacks the implemented IS measures failed to cope with. And then propose an algorithm to neutralize these threats.

1.5. Practical task

It is necessary to design a corporate computer network consisting of 100 hosts. When building a distributed branch infrastructure, the main servers should be hidden behind the NAT of the main office. When placing network equipment (L2+ switches, routers, firewalls, etc.), one should document the key settings which explaining the feasibility of using different protocols, technologies and intelligent features.

Then, you need to install and configure the gateway of the main office based on the server operating system (OS) Windows or Unix/Linux. In the benchmark analysis, the choice should be argued not only for the operating systems family, but also for a specific product. Key benchmark parameters: reliability/fault tolerance, information security, performance, maintenance complexity.
On the initial server configuration, you should pay attention to the following aspects:

1) backup and scalability;
2) organization and protection of remote access (protocols, technologies and authentication algorithms, etc.);
3) configure the firewall (including NAT and DMZ);
4) eliminating the published vulnerabilities and known tools hidden control computer (backdoors);
5) installation of additional defenses.

A number of interesting issues arise during the practical task implementation. Is it necessary to install an antivirus on an Internet gateway, and if so, which one? Whether the OS-integrated NAT implementation solutions meet the information security requirements?

Report content

1. Purpose of work.
2. Statement of work.
4. Installation and configuration of the server solution.
5. IS measures implementation.
6. Conclusion.

1.6. Control questions

Check yourself

What IS capabilities are implemented in managed network devices? Give examples.
What is the principle of access control lists? What are the differences between standard and extended lists? Give examples.
How can VLAN technology reduce the amount of broadcast traffic on the network?
Describe the working principle of simple network management protocol SNMP.
Give an example of the correct configuration of disk space. How can one ensure server fault tolerance and performance?
What is the working principle of the iptables packet filter? What is a connection tracer?
How are DNAT and SNAT technologies applied?
For what purposes is the creation of a demilitarized zone (DMZ) in the network? What dangers could this entail?
How is it preferable to organize remote network access? Explain your answer.
List the most common network attacks, their possible consequences and counteraction methods.
Distributed web systems and web application layer firewalls

Keywords: Web server, DBMS, server event handler, DNS, Geo DNS + API, HTTP, HTTPS, global cache, distributed cache, proxy, load balancing, queues, asynchronous processing, SSL, TLS, DDoS, SQL-Injection, XSS, Flash, JavaScript, PDF, XML, IFRAME, CSRF, brute force, phishing.

This chapter deals with the most common threats to the security of web resources and ways to neutralize them. Distributed denial-of-service attacks and their various variations are discussed in detail.

2.1. Web servers

A web server is a software whose main function is to receive and process requests from clients. In terms of a hardware perspective, a web server is a computer that stores site files and delivers them to the end user's device. The client is usually a web browser: it sends requests to the web server for receiving any resources (HTML pages, files, images, etc.), indicating their URL (Uniform Resource Locator), and receives the requested data in response. Data communication is carried out using the HTTP (HyperText Transfer Protocol) or HTTPS (HyperText Transfer Protocol Secure). There are static and dynamic web content. Static one contains unchanged text and multimedia information, while dynamic one is generated depending on user actions.

The functions of web servers include the following:
1) web pages automation;
2) search for database updates for various programs (antiviruses, torrent clients, etc.).
3) user authentication and authorization;
4) maintaining of call log to any resources.

As a next step, we consider the most common security threats to web servers.

2.2. The main security threats to web resources

Providing technical support for a web server, one has to deal with the following types of malicious influences in practice [17-36]:
1) Distributed Denial of Service attacks (DDoS) — bringing the computer system to failure through numerous distributed requests;
2) SQL injection. They are attacks aimed at web applications and allowing to modify the logic of executing SQL queries by injecting arbitrary SQL code into them;
3) Cross-Site Scripting (XSS) — attack using client-side scripting language vulnerabilities (JavaScript, Flash). It is done by substituting malicious code into the page generated by the server;
4) attacks based on the input of incorrect form data. In the case of setting insufficiently strict or incorrect checks of the input data, the attacker gets the opportunity to send one's own data. For example, this allow ones to fill the database with invalid records and then perform a DDoS attack, requesting a page that displays non-existent data;
5) exploitation of defects in the information resource code;
6) insufficient resistance to automation — the ability to automatically perform operations that should be performed manually. A standard example is systems of automated vulnerability search;

7) cookie files modification;

8) kidnapping sessions;

9) URL modification;

10) attacks based on "slow" HTTP requests (slow HTTP Post and slow HTTP Headers) — slow transmission of small portions of POST requests and HTTP headers to the server. The connection is not closed until the data transmission is complete. A large number of such connections leads to the exhaustion of server resources and its overload;

11) exploitation of vulnerabilities in cryptographic algorithms;

12) exploitation of web server and OS vulnerabilities.

One of the best-known of types of attack should be considered in greater detail — distributed denial of service attacks (DDoS).

This type of attack is the most common and effective, because there are no guaranteed methods of protection against them, and special knowledge for DDoS attacks is not required.

Structure of DDoS is hierarchical and usually consists of three levels: the management console, intermediate machines, and "infected" agents (Fig. 2):

![Fig. 2. Structure of DDoS attack](image)

The control console gives a signal about the beginning of the attack, then intermediate computers transmit the signal to agents, and they, in turn, send requests to the attacked node. Using such an attack structure almost completely eliminates the possibility of detecting its initiator.

The main types of DDoS attacks are described below.

**SMURF** — sending falsified Echo requests on behalf of the victim to the broadcast address of the network. All nodes that receive such a request send an Echo response to the node initiated the attack, resulting in the entire network to be overloaded due to a wave of response messages and there is denial of service, accordingly.

**SYN Flood** — sending numerous TCP connection requests with the attacked host. It leads to the depletion of the resources allocated to them to service future connections. As a result, the attacked node is in a locked state for a long time and is unable to accept new connection requests.

**UDP Flood** — sending multiple UDP messages to the attacked host. It leads to an increase in the load on the communication channel and overload of the attacked system.
**DISTRIBUTED WEB SYSTEMS AND WEB APPLICATION LAYER FIREWALLS**

*Ping-of-Death* — sending a fragmented ICMP packet larger than 64 KB to the attacked host, which can lead to an overflow of the network stack and the node to become incapacitated.

*Land* — sending a SYN packet to the attacked node with identical sender and receiver addresses, as a result of which the node falls into a loop of endless calls to itself.

*WinNuke* — sending urgent overhead data (Out of Band, OOB) to the attacked node for a TCP connection through port 139. It leads to the crash of the system (because Windows systems do not provide the ability to receive urgent data).

*Teardrop* — an attack based on the use of an error that occurs during the assembly of a datagram (an error of overlapping IP fragments). A datagram with false values of start and fragment length is sent to the attacked node, which causes memory errors and Windows system crash after its assembly.

Standard mechanisms to counter DDoS attacks are the use of captcha (CAPTCHA — Completely Automated Public Turing test to tell Computers and Humans Apart), setting a limit on the number of simultaneous connections, setting a limit on connection time and blacklisting.

It is necessary to independently disclose the details of the above attacks and explore methods to counter them, demonstrating the skills of searching, processing and analyzing information on the Internet.

### 2.3. Practical task

It is required to make a benchmark analysis of the software demanded in the market for the implementation of a web server. You should install the selected set of products based on the deployed server solution in the practical tasks of the first chapter (or a separate virtual machine). Then, configure it with the installation of additional defenses that neutralize the previously described threats. Don't forget that the keywords to each chapter always provide tips.

#### Report content

1. Purpose of work.
2. Statement of work.
4. Installation and configuration of the server solution.
5. IS measures implementation.
6. Conclusion.

### 2.4. Control questions

#### Check yourself

- What is a web server?
- What security threats may encounter a web server administrator?
- What are the dangers of slow HTTP requests?
- What are the standard ways to counter SQL injections?
- What is the classic structure of a DDoS attack?
- List the existing types of DDoS attacks and methods of countering them.
- How is cross-site scripting implemented?
- Give an example of cross-site request falsification.
- Why shouldn't PDF files be opened in a browser?
- What security software can neutralize the described threats?
3. Centralized file sharing technologies

A file server is a resource intended to perform file input/output operations and store files of any type.

The server is demanding on the amount of storage space and access speed. Accordingly, it is necessary to use RAID and LVM technologies to ensure uninterrupted operation and increased speed of data reading and writing.

In selecting disks, don't forget the following aspects:

1) SATA (Serial ATA) — a serial interface for data communication with information storage devices. The target group is personal computers and low cost server hardware. Compared to SAS and SSD drives, the read and write speed of SATA drives are noticeably lower. However, the advantage is a large amount of stored information.

   SATA drives are well suited for servers that don't require frequent writing and reading of information. For example, streaming operations:
   - video encoding;
   - data stores;
   - backup systems;
   - large file servers with low parallel load.

2) Serial Attached SCSI (SAS) is a serial computer interface designed to connect various mass storage devices (hard disks and tape drives). SAS is designed to replace the parallel SCSI interface and it uses the same set of commands.

   Ensuring high reliability of SAS data storage determines their purpose:
   - hosting;
   - Database Management System (DBMS);
   - high-load web servers;
   - distributed systems;
   - systems that process a large number of requests (terminal and 1C servers).

   The main disadvantage of SAS drives (similar to SSD) is their small capacity and high price.

3) Solid-state drive (SSD) — a computer non-mechanical storage device based on memory chips with a controller. Solid-state drives have smaller size and weight than traditional hard drives (SAS and SATA), but they have almost five times the cost per gigabyte and significantly low wear resistance (recording resource). It is worth listing the types of memory in ascending speed and cost indicators: MLC (Multi-Level Cell), TLC (Triple-Level Cell) and 3D NAND.

   SSDs have no moving mechanical components, which provides high mechanical resistance, reduced power consumption and high speed operation. At the moment, SSD drives provide the highest possible read and write speed, which allows them to be used for almost any high-load projects.
The most popular form factors: 2.5", mSATA, M.2, PCI-E. It is also worth highlighting the new logical interface *NVM Express*, designed specifically for solid-state drives. It differs from the old *AHCI* with lower latency and high parallelism of memory chips due to a new set of hardware algorithms.

For each server object, you can choose a secure variation of the *FTP* server that would suit your corporate computer network project. The market offers a wide range of software: *wu-ftpd*, *ProFTPD*, *Pure-FTpd*, *SlimFTpd*, *vsftpd*, *Internet Information Services*, *glFTPd*, *CrushFTP Server*, *GoAnywhere Services*, *Cerberus FTP Server*, *FileZilla Server*, etc.

An acceptable decision may be *NAS* technology (*Network Attached Storage*). It is a high-performance server or a cluster of servers with a disk array connected to the network and supporting the work on the protocols accepted in it. Of course, there is support for *RAID*-arrays. *NAS* is characterized by reliability of data storage, ease of access to users, ease of administration, scalability.

It is worth distinguishing a similar implementation with *SAN* technology (*Storage Area Network*), which is an architectural solution for connecting external storage devices so that the operating system recognizes connected resources as local.

### 3.2. Decentralized File Sharing Technologies

An alternative is *BitTorrent* — a network protocol for cooperative peer-to-peer file sharing (decentralized, *P2P*) over the Internet. Files are transferred in blocks. Each *torrent* client, receiving (or downloading) these parts, at the same time, gives (or uploads) them to other clients, which reduces the load and dependence on each source client and ensures data redundancy.

Let's consider the working principle of the protocol in more detail.

To download a file, the client connects to the *torrent tracker* — the server that connects *BitTorrent* clients to each other, and transfers its *IP* address and the checksum of the file to download. Then, from the tracker, he receives the *IP* addresses of other clients who download or upload the torrent file; the list of *IP* addresses is regularly updated during the download process.

Data is transferred between clients without the direct participation of the torrent tracker: it only collects information about the download process, connected clients, etc. Clients exchange information about segments of the file stored by them after the connection is established. A client wishing to download a file sends a download request, receives a segment in case the second client is ready, and then compares the checksum of the fragment with the amount recorded in the torrent file. In a case of amounts match, the download is considered successful, and the client notifies other clients that he has a fragment of the file.

In order to optimize distribution, the client can suspend the transfer of torrent file fragments to another client: priority is given to the node that itself transmitted the largest number of segments.

Using this technology has a number of advantages:

1) no waiting to download;
2) downloaded fragments are instantly available to other users;
3) the integrity of each fragment is monitored;
4) the distribution object can be several files (for example, the contents of the directory);
5) high download speed, growing with increasing number of clients.

Newer protocol versions perform the possibility of file distribution without a tracker using a *distributed hash table* *DHT*, which solves the failure problem of the entire network when the tracker fails. Also, work without a torrent tracker is possible when using multi-protocol clients with *BitTorrent* support; for example, the *Shareaza* client exchanges *IP* addresses of nodes of other supported networks, including *BitTorrent*, through the *Gnutella2* network.

In addition to *BitTorrent*, there are many other implementations of file-sharing networks: *Direct Connect*, *Gnutella*, *Gnutella2*, *FastTrack*, etc.

Also, do not exclude from the analysis the *cloud storage* — an online storage model in which data is stored on numerous network-distributed servers configured using virtualization technologies.

It will be necessary to work out the correct multi-user mode of operation after choosing the technology of file-sharing network access. The next important stage is testing objects in an information security environment.
3.3. Practical task

First of all, it is necessary to master the theoretical part of the material [37-41] and study the existing technologies of file-sharing network access. Then perform a search and benchmark analysis of existing solutions (both free and proprietary). Deploy the most cost-effective solution to a previous or new virtual machine, or present it as a project. Install additional modules to protect against external malicious influences. Perform an IS audit of the deployed server solution. Illustrate the correct multi-user mode of operation. Analyze possible vulnerabilities of the object.

Report content

1. Purpose of work.
2. Statement of work.
5. Implementation of the selected project.
6. Testing the server solution.
7. IS measures implementation.
8. Conclusion.
9. References.

3.4. Control questions

Check yourself

- What is a file server? What advantages does it have?
- For which servers is it preferable to choose SATA, SAS or SSD drives?
- What are the implementations of FTP servers that you know? Give their benchmark analysis.
- What is NAS technology? What is its difference from SAN?
- Describe the principle of peer-to-peer (P2P) operation networks.
- What are the advantages of P2P technology over centralized file sharing?
- What is the principle of the BitTorrent protocol?
- List known file sharing network implementations besides BitTorrent. Give their significant differences.
- What are the features of cloud storage?
- What vulnerabilities are considered data storage technologies?
Basics of administration of centralized work of users in distributed systems

Keywords: 1C: Enterprise, terminal server, application virtualization, rich and thin clients, web interface, DBMS, MySQL, MS SQL, PostgreSQL, web server, ssl, https, Remote Desktop Services, Terminal services, RDMS, Application Virtualization, Active Directory, DNS, DHCP, VMware Horizon, VMware View, gold-iso, PCoIP, print server, screwdrivers.

This chapter focuses on technologies to provide centralized work of users with applications. Material about virtualization, terminal server, domain controller is stated.

As an example, consider one of the most popular products in Russia, which requires a centralized work of users. It is 1C Enterprise, a software product of the 1C company, designed to automate the activities of the enterprise. It is able to work through rich and thin clients, a web interface. In the first option, processing of information is performed mainly on the local-side, and when dealing with a thin client or web interface, it is on the server-side. The latter mode of operation does not require large resources of both the system and the communication channel. At the same time, don't forget about the safety of interconnection. For example, https should be used instead of http.

There are a lot of options for building a system of centralized user work with applications [42-45]. Modern standards of information technologies allow to refuse desktop computers, because installation, maintenance, software updates on each system unit are a time-consuming task. Now computational power is far ahead of software requirements. This gave rise to the era of virtualization. Consider the main options for solving the problem: terminal server, application virtualization, Active Directory.

4.1. Terminal server

Terminal server — a server that provides clients with computing resources (CPU time, memory, disk space) to solve problems. Technically, a terminal server is a very powerful computer (a computing cluster) connected to terminal clients via a network. The latter are subject to minimum system requirements. The terminal server is used for remote maintenance of the user or administrator with the provision of a desktop or console.

The terminal server is referred to Remote Desktop Services in Microsoft terms. Clients get access to the Windows Server desktop or to the application (RemoteApp) using the Remote Desktop Protocol (RDP), http, https. Over a hundred of users can work on one terminal server simultaneously and in isolation. With this approach, there is a saving of computing resources allocated per user, in comparison with the complete virtualization of individual operating systems (VDI RDS, Virtual Desktop Infrastructure).
4.2. Application virtualization

There is a technology of application virtualization. For example, *Microsoft Application Virtualization (App-V)* allows each application to run in its own standalone virtual environment on the client machine. Virtualized applications are isolated from each other. This avoids conflicts between applications, but they can still communicate with the client machine.

Such technologies are not an innovation. The market of virtualization successfully mastered the product *Citrix XenApp* more than a decade ago. However, today the leader is *VMware, Inc.*

This company coined the term *VDI — Virtual Desktop Infrastructure* to position its personal computer virtualization technology. But the corporation also deals with application virtualization. *VMware* implemented *View, ThinApp* products. These are tools for creating an enterprise virtual PC infrastructure and application virtualization with wide functionality in the field of automatic deployment and maintenance.

*VMware Horizon* project received development. It is an integrated solution that provides access to published applications and desktops based on a single platform. Enterprise applications and operating systems are centrally managed by using *Horizon*.

The following technical aspects of *Horizon* should be noted:

1) access to published applications and virtual desktops based on a single platform offers simplified management, granting rights to end users and fast delivery of published applications, desktop computers, remote and virtual desktops to various devices and locations;

2) unified workspace for simplified access — end users can get access to all applications and desktops from a single unified workspace.

3) storage system optimization and delivery from a software-defined data center;

4) closed cycle of control and automation. Ensuring operational status monitoring and risk monitoring, proactive monitoring of end-user behavior and in-depth diagnostics from the data center to the device inside a single console;

5) centralized images management of virtual, physical and personal devices of employees;

6) access to the hybrid cloud.

4.3. Active Directory

Not less interesting project is *Active Directory (AD)*, an *LDAP*-compliant implementation of *Microsoft*'s directory service for the *Windows NT* family of operating systems. *Active Directory* allows administrators to:

1) use *Group Policies* to ensure uniformity of users work environment;

2) deploy software on multiple computers through *Group Policies* or through *System Center Configuration Manager* (formerly *Microsoft Systems Management Server*);

3) install updates to the operating system, application and server software on all computers on the network using the *Windows Server Update service*.

*Active Directory* stores data and environment configuration in a centralized database. *AD* networks may be of different sizes: from a few tens to a few million objects. Network resources, information about which is stored in the database, in *Active Directory* terminals are called objects and are separate named sets of attributes. Attributes depend on the type of object and represent the characteristics and data that may be contained in it (Fig. 3):
**Active Directory** can be viewed in terms of logical and physical structures. The logical structure defines a lot of objects that can be stored in a directory: for each object class, mandatory and additional attributes of its representatives are specified, as well as which object class can be a parent in relation to this one.

The logical structure includes the following components:

1) organizational units — logical containers that allow to group objects;
2) domains — the basic structural unit of Active Directory;
3) domain trees — a system of domains that has a hierarchical structure and a single root (root domain);
4) domain forests — a set of domain trees that are in some form of trust relationship.

The hierarchy of AD logical components is shown in figure 4:
Because the logical structure of AD is independent of the physical location of servers and network connections in the domain, when planning it, the hierarchy of domains is determined independently of the requirements of the physical network, taking into account only administrative and organizational requirements.

The physical structure of Active Directory includes nodes (sites) and domain controllers, and reflects the physical structure of the organization. The purpose of planning the physical structure of AD is to optimize replication — the process of copying changes made on any one of the domain controllers, to all controllers. The site is part of a network in which all domain controllers are connected by high-speed communication lines. Connections between the sites themselves are slower. This structure is explained by the need for frequent replication within sites with the ability to transfer large amounts of data without compression, whereas this process is less frequent between sites, and the transmitted data should be compressed (Fig. 5):

![Fig. 5. Active Directory physical structure](image)

Because logical and physical structures serve different purposes, they are virtually unrelated: their common object is the domain controller that stores the Ntds.dit catalog file, which contains information about both structures.

### 4.4. Practical task

It is necessary to satisfy customer requirements — to introduce a 1C:Enterprise server in our distributed corporate network so that each user can work in this program without being tied to one's workplace. Under similar conditions, all users will have to interact with other accounting applications and submit timely reports — both in electronic and printed form.

After getting acquainted with the theoretical material, it is necessary to conduct a benchmark analysis of existing technologies and products. Develop and realize the project for implementing the selected solution in a test corporate computing network. As an example, you should use the introduction of 1C:Enterprise and any other related accounting applications. One should consider printing from remote objects, improve the safety layer by implementing an event and security management system, and conduct the final testing of the implemented complex of ICT protection. An additional advantage will be the use of intrusion detection and prevention systems.

---

Report content

1. Purpose of work.
2. Statement of work.
5. IS measures implementation.
7. Conclusion.
8. References.

4.5. Control questions

- What are the purposes of the product 1С:Enterprise? What are its functioning modes?
- List the mechanisms for data security provided in 1С:Enterprise.
- What is a terminal server? What advantages and disadvantages does it have?
- Describe the conceptual basis of application virtualization technology.
- What are the capabilities of VMware Horizon?
- What is Active Directory used for?
- How is Active Directory related to the domain name system?
- Define the concept of an object, an attribute in terms of AD. How are they interconnected?
- What are the purposes of building the logical and physical structures of AD?
- Give the main components of the logical and physical structures of AD. How are these structures interconnected?
5.1. Theoretical bases of vulnerability analysis of information systems and computer networks

When performing security testing of computer networks and information systems, it is impossible to do without network traffic analyzers (sniffers). This term is defined as a program or a hardware-software device designed to intercept and subsequently analyze or only analyze network traffic. For the sniffer to work correctly, it is necessary to configure the network interface in the "promiscuous mode" in order to process all network segment traffic.

Vulnerability scanners are another important tool. These are software or hardware and software tools used to perform diagnostics and monitoring of network hosts, allowing you to scan networks, computers, and applications for possible security problems, find and fix vulnerabilities. It should be noted that most software products only issue instructions for fixing vulnerabilities or using them.

Scanners identify the following typical vulnerabilities:

1) incorrect configuration of firewalls, network equipment, web servers and databases;
2) previously published and well-known tools for stealthy computer management (backdoors);
3) susceptibility to penetration from unprotected systems;
4) trojan software;
5) weak passwords.

Such tools can be network-based, host-based and application-based. The most widely used are security analysis tools for network services and protocols. The second-most used are OS security analysis tools.

In addition to detecting vulnerabilities using security analysis tools, you can quickly identify all the nodes of the corporate network that are available at the time of testing, identify all the services and protocols used in it, their settings and the potential for unauthorized impact (both inside and outside the corporate network).

There are two main mechanisms by which a scanner checks for vulnerabilities. This is scanning and probing.

Scanning is a passive analysis mechanism by which the scanner tries to determine the presence of a vulnerability without actually confirming its presence by indirect signs. This method is the fastest and simplest to implement.
Probing is an active analysis mechanism that allows to verify whether a vulnerability is present on the node being analyzed. Probing is performed by simulating an attack that exploits the vulnerability being checked.

5.2. Vulnerability analysis tools

These mechanisms are quite often implemented by the following methods [46-51]. First of all, banner check is used. This mechanism is a series of scan-type checks and allows to make a conclusion about the vulnerability, based on the information in the response header to the scanner request. A typical example of such a check is an analysis of the Sendmail program or FTP server headers, which allows to find out their version and on the basis of this information to conclude that there is a vulnerability. The described method to implement checking for the presence of vulnerabilities on the scanned node is the fastest and easiest.

Secondly, active probing checks are used. They also relate to the scanning mechanism. However, they are not based on software version checks in the headers, but on a comparison of the software fragment’s digital fingerprint and the fingerprint of a well-known vulnerability. Antivirus systems also use a similar method by comparing the fragments of software being scanned with virus signatures stored in a special database. This method has a good speed, but is more difficult to implement than checking headers.

And in conclusion, exploit check is applied. These checks relate to the "probing" mechanism and are based on the exploitation of various defects in the software. A special case of probing is pentest (penetration testing).

Most scanners perform security analysis in several steps:
1) gathering information about the network. At this step, all active devices in the network are identified, and the services and daemons running on them are determined;
2) detection of potential vulnerabilities. The scanner uses a database to compare the collected data with known vulnerabilities by checking headers or active probing checks;
3) confirmation of the selected vulnerabilities. The scanner uses special methods and models/simulates certain attacks to confirm the presence of vulnerabilities on selected network nodes;
4) report generation. The security analysis system generates reports describing detected vulnerabilities based on the collected information;
5) automatic elimination of vulnerabilities or giving instructions on their neutralization or use. This step is very rarely implemented in network scanners, but is widely used in system scanners.

The most informative products in this area are highly specialized software solutions from hackers that describe and exploit previously unknown and not officially published vulnerabilities. However, they can often be found only using overlay networks. Accordingly, it is necessary to demonstrate the skills of searching, processing and analyzing information.

Any information resource requires support by a qualified technical specialist to ensure the appropriate level of information security. This is necessary to eliminate various problems, carry out maintenance work, update software, study and eliminate zero-day vulnerabilities.

One of the most common operating systems in the field of information security is Kali Linux. This distribution, which came to replace the OS for BackTrack security testing, is based on Debian GNU/Linux. Kali Linux is a specialized tool and is not intended to be used as a main distribution: it lacks most of the services and programs necessary for solving everyday tasks.

Kali Linux contains the following categories of programs:
1) network scanners — programs that determine the configuration of systems, open ports and the services running on them, and identify known vulnerabilities;
2) sniffers that intercept network traffic;
3) the Exploit Database — databases that include a large number of ready-made programs for using known software and OS vulnerabilities;
4) password guessing software (brute force);
5) proxy toolbox (these tools are discussed in more detail in the chapter 9: "Anonymization on the Internet");
6) Cisco toolbox;
7) wireless network utilities;
8) web toolbox;
9) database tools, etc.

Let's list the most popular:

1) John The Ripper (JTR, John) — an open source program that allows guessing passwords (brute force). The working principle of JTR is to encrypt text strings from a dictionary similar to password encryption and compare the result with it.

2) Aircrack-ng is a set of tools for testing the security of wi-fi networks. It makes it possible to monitor network traffic, brute-force the WPA-PSK keys, etc.;

3) THC Hydra — a tool that works similar to JTR, but online;

4) Burp Suite — a program for vulnerability scanning on web sites and applications;

5) Wireshark — network traffic analyzer;

6) Nmap — a program for testing network security and port scanning;

7) Maltego — an analytics tool that allows to find and visualize the communication between events and objects;

8) Metasploit — a set of tools for testing known vulnerabilities;

9) Acunetix — a website scanning program that allows to detect probable SQL injections, XSS, CSRF, etc.;

10) Social-Engineer toolkit — a tool for testing social engineering attacks.

It should be noted that all considered programs and utilities are put to good use. This chapter is focused on developing your skills in the field of information security and is not a guide for unauthorized entry.

5.3. Practical task

First of all, it is necessary to master the theoretical part of the material and study algorithms, methods and tools for testing information security of computer networks and information systems. Then perform a search and benchmark analysis of existing solutions (both free and proprietary). Next, audit the information security of a previously deployed server solution using the tools considered. Analyze and eliminate the identified vulnerabilities of the object.

Report content

1. Purpose of work.
2. Statement of work.
4. Testing the server solution.
5. IS measures implementation.
6. Conclusion.
7. References.

5.4. Control questions

Check yourself

What are network traffic analyzers?
What are vulnerability scanners? What standard vulnerabilities can they identify?
What information can scanners identify in addition to vulnerabilities?
At what layers are vulnerability scanners capable of operating? What are the differences?
List the vulnerability detection mechanisms used by the scanners. What are the methods of their implementation?
Give an example of a phased analysis of the security of an information system or network.
Give examples of software products for performing vulnerability analysis (both free and proprietary). Why is it recommended to use overlay networks to find them?

Why is it not recommended to use Kali Linux for everyday tasks?

What kinds of programs are contained in the Kali Linux distribution?

List distributions for information security testing, in addition to Kali Linux. What are the differences?
This chapter is devoted to the study of intrusion detection and prevention systems, as well as events collecting and correlating systems. The architecture, functions, algorithms and methods of these systems operation are considered.

6.1. **IDS/IPS architecture and features**

*Intrusion Detection System (IDS)* are software or hardware/software systems that automate the process of viewing events occurring in a computer system or network and analyze them in terms of security [52-56]. This definition can be considered correct in the framework of the theory of computers, systems and networks.

*IDS* consist of three functional components: information sources, analysis and response. The system receives information about the event from one or more information sources, performs an analysis of the event data, determined by the configuration, and then creates special answers — from simple reports to active intervention in detecting penetrations.

Intrusion detection is the process of monitoring and analyzing events occurring in a computer system or network.

Intrusions are defined as attempts to compromise the privacy, integrity, availability, or bypassing security mechanisms of computer or network. Intrusions can be carried out both by attackers accessing systems from the Internet and by authorized users of systems trying to gain additional privileges that they do not have.

There are the most common intrusion detection system features:

1) anticipatory action with a warning about responsibility;
2) filtering information streams;
3) identification of attack preambles (network probing or some other testing to detect vulnerabilities and prevent their further development);
4) documenting existing threats to the network and systems;
5) ensuring quality control of development and administration;
6) obtaining useful information about intrusions that have occurred, with the provision of improved diagnostics to recover and correct the factors that caused the intrusion;
7) identification of the intrusion side.

*Intrusion Prevention System (IPS)* is called *IDS* with automatic protection tools. In addition to batch processing in modern products, there is often a mode of operation in *Real Time*.

6.2. **Types of IDS/IPS**

Intrusion detection and prevention systems can operate the network, host and application layers. *Network-based IDS/IPS systems* consist of many information sources (sensors) located at key points in the network (Fig. 6). They have a number of advantages:
1) the proper location of several NIDS/NIPS allows to view a large network. NIDS/NIPS data acquisition sensors should be installed in each network segment (e.g. through mirroring technology on managed L2+ switches);
2) NIDS/NIPS do not affect the normal operation of the network, so their placement does not require modification of its topology;
3) NIDS/NIPS can be placed in an invisible way to an attacker.

However, such systems have the following disadvantages:
1) attack detection can be difficult with high traffic volume in large or busy networks;
2) the inability to analyze information transmitted in encrypted form (if there are no certificates and keys for the decryption procedure);
3) NIDS/NIPS are difficult to identify network attacks that include fragmented packets.

Fig. 6. Network-based IDS/IPS

Host-based IDS/IPS (HIDS/HIPS) analyze system log entries and OS audit results, tracking attacks directed to a specific host (Fig. 7).

Fig. 7. Host-based IDS/IPS

Compared to network intrusion detection and prevention systems, HIDS/HIPS have the following advantages:
1) HIDS/HIPS are able to detect attacks that NIDS/NIPS do not see because the analysis of security events is locally focused on a single node;
2) Often HIDS/HIPS are able to work in encrypted network traffic;
3) HIDS/HIPS operation does not depend on the presence of switches and other network devices in the network, unlike NIDS/NIPS.

There are disadvantages of HIDS/HIPS:
1) **HIDS/HIPS** are configured for each node separately, so these systems are more complicated to configure and manage;
2) Due to the location on the potentially attacked host, **HIDS/HIPS** themselves can also be attacked;
3) **HIDS/HIPS** do not have the ability to detect scans of the entire network, because they analyze packets received by a particular host;
4) **HIDS/HIPS** can be blocked by some types of DoS attacks;
5) **HIDS/HIPS** consume the computing resources of monitored hosts.
6) due to the use of a large amount of data (OS audit results) of **HIDS/HIPS**, additional local storage of information may be required.

Application-based IDS/IPS can generally be called a subset of **HIDS/HIPS**. They interact directly with the application and analyze the events received in its software.

There are the advantages of these systems:
1) **application-based IDS/IPS** are able to track user unauthorized activity by analyzing their interaction with applications;
2) **application-based IDS/IPS** are able to operate in environments with encrypted traffic.

These systems have the following disadvantages:
1) **application-based IDS/IPS** can be vulnerable in case of an attack on application logs, because they are often not as secure as the OS audit results used by host-based **IDS**;
2) **application-based IDS/IPS** are unable to detect attacks related to software integrity violations (trojans, etc.).

### 6.3. Security Event Analysis Approaches

It is worth highlighting the main methods of operation of intrusion detection and prevention systems: signature-based, behavior-based, anomaly-based, and combined.

Signature-based detection uses an analysis of the correspondence of system security event to a given pattern describing a known attack. This method is very effective at detecting known attacks and means of their implementation, moreover, it does not depend on qualification of the system administrator. However, a significant weakness of defining abuses is the inability to identify attacks whose signatures are not in their database, as well as complex combined attacks.

Anomaly-based detection is a determination of the unusual user and system behavior. Based on the history data, profiles are created that describe the standard activity of users or hosts, and then, using a number of metrics — statistical, neural networks, genetic algorithms — the deviation of the analyzed behavior from normal is determined. The identification of anomalies, in contrast to the signature-based method, allows to identify previously unknown attacks without knowing their details, however, this method creates a large number of false positives in case of unpredictable network activity. In addition, it requires time-consuming training of the security system to determine indicators of normal behavior. Behavioral analysis is often considered a synonym for the anomaly-based detection, although it is customary to distinguish these concepts in the scientific literature.

In addition to the described intrusion detection methods, own system security policies should be mentioned. The description of network security rules requires high professional training from the administrator and is a more time-consuming process than the use of standard methods of system event analysis. However, this approach is the most flexible and allows to detect new attacks. The combination of signature-based method, anomaly-based method and application of security policies will significantly improve network security. It is worth noting that these methods don't live up to expectations in real systems that use cryptographic protocols and overlay networks.

One should not forget that there are **Security Information and Event Management (SIEM)** systems for complex information security. The functional purpose of this tool is to analyze information coming from various systems (OS, antivirus, scanning and filtering programs, DLP, IDS/IPS, routers, firewalls and other applications/network nodes), as well as to detect deviations from the norms of various parameters. If a deviation is detected, the system generates an incident. Statistical and mathematical technologies are an
integral part of SIEM’s work. These systems allow to control the requirements of regulatory documents and security policies, detect attacks in a timely manner and respond to them quickly. In addition, SIEM can solve a number of common problems that a network administrator may encounter:

1) SIEM systems collect event data from virtually any information sources and bring them to a uniform view, which simplifies the task of analyzing security events;
2) SIEMs are able to aggregate events that are similar, thereby reducing the amount of data for analysis without losing potentially important incidents;
3) SIEMs allow to detect complex distributed attacks by matching events that may seem unrelated at first glance;
4) SIEMs solve the problem of centralized storage of events of various systems using compression.

An important aspect of corporations implementing SIEM is the time spent collecting statistics on normal node behavior. Test operation of these systems can last for several months, with most of the positives will be false during this period. Thus, it is necessary to clearly realize that the installation of security information and event management systems to improve network security is necessary in the case of a large distributed network infrastructure, the presence of a large number of network information security devices (firewalls, intrusion detection and prevention systems, DLP systems, antiviruses, etc.), the presence of specific devices in the network infrastructure, requirements for compliance with various standards, and the frequent need for investigation incidents (for example, when detecting more than one hundred attempts to penetrate from the outside per day).

### 6.4. Practical task

After getting acquainted with the theoretical material, it is necessary to conduct a benchmark analysis of existing intrusion detection and prevention systems. Develop and realize a project for implementing the selected product into a test corporate network. Explore the algorithms and methods of operation of these systems by launching the mechanisms of active and passive analysis of objects (scanners, sniffers, probes). Improve the safety layer by implementing security information and event management system. And conduct the final testing of the implemented ICT protection complex.

**Report content**

1. Purpose of work.
2. Statement of work.
4. IS measures implementation.
5. Testing the implemented ICT protection complex.
6. Conclusion.
7. References.

### 6.5. Control questions

**Check yourself**

- What is an intrusion detection and prevention system (IDS/IPS)?
- What features do these systems include?
- Describe the architecture of IDS/IPS systems.
- At what layers are IDS/IPS systems capable of operating? What are the differences? What are their advantages and disadvantages?
- What is the difference between this class of systems and firewalls?
- List methods for analyzing security events in intrusion detection systems.
- Which of these methods is the best? Explain your answer.
- What is a security information and event management system (SIEM)?
Give primary features of SIEM systems.
Can this system replace IDS/IPS? Explain your answer.
Software cryptographic mechanisms of information protection

Keywords: symmetric and asymmetric encryption, PGP, OTR, GPG4WIN, XMPP, Tox, TrueCrypt, AxCrypt, DiskCryptor, FreeOTFE, BestCrypt.

This chapter focuses on the study of cryptographic information protection tools. Basic theoretical information about cryptography and cryptographic algorithms is provided.

Information security specialists are required to work with legal documents of both the Russian Federation and international ones. The theoretical part contains excerpts on key definitions of the area in question for gaining experience with state terminology.

Cryptography is a discipline that includes the principles, tools and methods of converting information in order to conceal its content, prevent its undetectable modification or unauthorized use. Cryptography is limited to converting information using one or more secret parameters (such as cryptographic variables) or appropriate key management.

Cryptographic protection of information (encryption, decryption) is the process of converting open data in order to keep it secret from unauthorized persons using some algorithm called a cipher. The cryptographic conversion algorithm is used to encrypt information by the sides. It is implemented in a certified cryptographic information protection tool. Decryption is the reverse of encryption process.

Encryption facilities are hardware, software and hardware-software encryption (cryptographic) tools that implement cryptographic information conversion algorithms to limit access to information, including when it is stored, processed and transmitted.

Cryptographic Information Protection Facilities (CIPF) — hardware and/or software, certified in the manner prescribed by the legislation of the Russian Federation. They provide encryption, integrity control and the use of electronic signature in the exchange of electronic documents.

Electronic digital signature (EDS) — a sequence of characters obtained as a result of a cryptographic conversion of the source information, which allows to confirm the integrity and immutability of this information, as well as its authorship.

Technical protection of confidential information means the performance of work and/or the provision of services to protect it from unauthorized access, leakage through technical channels, as well as from special influences on such information in order to destroy, distort it or block access to it.

Authentication — the process of verifying that a subject has access rights to information resources in accordance with the presented identifier;

Symmetric algorithm — a cryptographic algorithm that uses the same key for both encryption and decryption. When using a symmetric algorithm, information exchange is as follows:
1) the sender passes the key to the recipient;
2) the sender encrypts the message sent to the recipient using the key;
3) after the message arrives to the recipient, one decrypts it.

Asymmetric algorithm — a cryptographic algorithm that uses a mathematically-related key pair for encryption and decryption. The steps of information exchange using this algorithm are as follows:
1) the receiver computes the public and private keys; the private key is kept secret, while the public one is publicly available;
2) using the recipient’s public key, the sender encrypts the message sent to the recipient;  
3) the message arrives to the recipient and is decrypted by one using a private key.

Unfortunately, the legislation of the Russian Federation is incomplete in the field of information technology. Even in the above definitions there are a number of inaccuracies, correcting which you can improve the final score for completing the task.

Let's consider two approaches to providing cryptographic information protection that should be applied in the course of the practical task to this chapter — local and remote [57].

7.1. Local approach to cryptographic information protection

An important aspect that requires attention is the potential for data interception and equipment theft. Unfortunately, setting passwords (BIOS, OS, archives, office documents), using standard encryption do not provide the appropriate level of information resources security and can be eliminated by a technical specialist in a matter of minutes. Accordingly, it is necessary to use cryptographic tools to protect the system partition/drive.

The most popular encryption tool "on-the-fly" (automatic encryption or decryption of data during reading/writing) is TrueCrypt. The TrueCrypt program has a wide range of features:
1) create an encrypted virtual disk in three different ways: in the container file, which greatly facilitates the work with it (transfer, copy, rename, etc.); as an encrypted disk partition; by fully encrypting the contents of the device (for example, USB flash memory);
2) providing two levels of plausible denial of encrypted data: it is possible to create a hidden volume and set a second password for a regular volume in order to gain access to data inaccessible by the master password;
3) the inability to identify TrueCrypt volumes — TrueCrypt volumes are indistinguishable from a random data set, therefore the files created by the program cannot be associated with it;
4) support for symmetric block encryption algorithms AES, Serpent and Twofish;
5) the ability to select one of three hash functions: HMAC-RIPMED-160, HMAC-Whirlpool, and HMAC-SHA-512 to generate encryption keys, modifier, and header key.
6) portability — TrueCrypt can be run without OS installation;
7) the ability to change passwords and passphrases to access volumes without losing encrypted data;
8) support for creating an encrypted dynamic file on NTFS drives (New Technology File System);
9) the ability to back up and restore volume headers (for example, if one needs to mount a volume after a hardware error that corrupted the volume header);

Currently, this software product is no longer supported by developers. The most trusted version is TrueCrypt 7.1.

In addition to TrueCrypt, there are many programs with similar functions on the market: BitLocker, AxCrypt, DiskCryptor, BestCrypt, FreeOTFE, etc. During the task, you need to conduct a benchmark analysis of these tools and make a reasoned choice of the most suitable of them.

7.2. Methods and tools of information security remote interaction

The remote approach to providing cryptographic information protection means ensuring the information security of remote communication using encryption technologies. As an example, the Extensible Messaging and Presence Protocol (XMPP) may be cited. This protocol is based on an eXtensible Markup Language (XML). The XMPP architecture is similar to other application layer protocols: each client has a unique name and exchanges information with other clients through the server. Communication between the client and server is encapsulated in XML streams. Another valid solution for instant messaging
is Tox. Peer-to-peer data exchange is used to ensure customer interaction. After installing Tox, a key pair is created: public key, serving as a unique identifier for the interlocutor, and private one, stored exclusively with the owner and confirming its authenticity. The search for interlocutors is performed using a distributed hash table. Connection protection is provided by using SOCKS proxy servers; in addition, there is the possibility of redirecting traffic through the Tor overlay network (it is discussed in more detail in Chapter 9: "Anonymization on the Internet").

It is important to understand that the use of these protocols in a standard form does not guarantee a sufficient level of security of the transmitted data, so the use of additional cryptographic tools is recommended.

It is possible to use a cryptographic protocol OTR (Off-the-Record) that provides encryption for instant messaging. This protocol satisfies three basic requirements: encryption of the transmitted data, authentication of the sides and the absence of the possibility of compromising correspondence in case of loss of keys. The latter is achieved by constantly updating keys during messaging. The Diffie-Hellman (DH) protocol is used to establish a shared private key. It allows two or more sides to obtain a common private key using an insecure communication channel, further using it to encrypt information exchange. Encryption in OTR is provided using the AES (Advanced Encryption Standard) algorithm. A key is used to authenticate messages obtained by hashing the key. It is used to encrypt a message.

This protocol is intended for use by only two sides. If it is necessary to use the protocol simultaneously by several users, it is possible to install the OTR extensions — GOTR (GroupOTR) and mpOTR (Multy-Party OTR).

Do not forget about the cryptographic system PGP (Pretty Good Privacy). This tool allows one to perform operations of encryption and digital signature of messages, files and other data presented in electronic form, including transparent data encryption on storage devices, for example, on a hard disk.

### 7.3. Practical task

The customer’s requirements are to prepare the director’s laptop and smartphone before business travel, as well as to consider the issue of one's secure communication with both staff and third-party opponents. According to the available data, competitors will attempt to intercept confidential information.

First of all, it is necessary to configure the objects: laptop and smartphone. One should prohibit all types of remote access, configure a firewall, eliminate vulnerabilities and backdoors, and install additional defenses (IDS/IPS, AV, etc.).

Next, it is necessary to use cryptographic tools to protect the system partition/drive. When making any decision, one have to conduct a benchmark analysis of existing products.

It is also inevitable to use encryption technology to protect the data transmission process. The chosen algorithms, methods and protocols should have a high level of cryptographic security. Two issues need to be considered: instant messaging between employees through an enterprise server and with opponents through third-party services and software.

Free open source software is more trustworthy than proprietary solutions.

**Report content**

1. Purpose of work.
2. Statement of work.
4. IS measures implementation.
5. Conclusion.
6. References.
7.4. Control questions

What is cryptography? Why is cryptographic information protection necessary?
Define "electronic digital signature" (EDS). What is it used for?
What are the symmetric and asymmetric data encryption algorithms?
Explain the need for additional encryption tools for system partitions/drives.
List the capabilities of providing cryptographic information protection implemented in the TrueCrypt software product.
What is meant by providing two levels of plausible deniability of encrypted data?
What TrueCrypt analogues do you know? What are the differences?
Give significant differences between OTR and PGP.
What tools can one use for instant messaging? Explain your answer.
What additional defenses can be installed for a laptop or smartphone?
This chapter is devoted to the study of virtualization technologies. Theoretical information about various virtualization methods and analysis of existing solutions in this area are provided. Working principles, mechanisms for processing requests to hardware resources and mechanisms for controlling them, and also distinctive features of each system are considered.

8.1. Theoretical Foundations of Virtualization Technologies

Virtualization is the provision of a set of computing resources or their logical combination abstracted from the hardware complex, and provided logical isolation of computing processes performed on a single physical resource [58-59].

Paravirtualization is a virtualization technology using a modification of guest operating systems. In turn, guest objects interact with the hypervisor program that provides the API, instead of directly using hardware resources. The hypervisor provides separation and management of resources provided by the guest OS, as well as ensuring the interaction of running OS and their isolation from each other. Changes to the guest OS for the hypervisor was previously possible only if it had open source code, but present-day systems do not have such a disadvantage. The virtualization method allows to achieve performance close to the performance of a real system.

Hardware virtualization is implemented with support for a special processor architecture. This technology makes it possible to use isolated guest systems that are independent of the implementation of the virtualization platform and are directly controlled by the hypervisor. The use of hardware virtualization also provides performance comparable to that of a non-virtualized machine. The most popular virtualization technologies are Intel-VT (Intel Virtualization Technology) and AMD-V.

Consider software programs that implement the described technologies: VMware ESXi, MS Hyper-V, OpenVZ, KVM.

8.2. Virtualization Software

The most famous hardware hypervisor is VMware ESXi, which is shipped as component of VMware vSphere. It is installed directly on a physical server, without requiring an OS installed on it, and divides it into several logical partitions (virtual machines). The advantages of this product are ease of deployment, configuration and management, as well as its small memory size. VMware ESXi is controlled using APIs, which makes it possible to monitor equipment and control the system without installing agents. In addition, remote command line interfaces — vSphere Command Line Interface (vCLI) and PowerCLI — are provided to implement system configuration and troubleshooting. Support for several deployment methods is implemented: using the ESXi installer, scripts, and the PXE environment (Preboot eXecution Environment). There is a scripting mechanism that is provided to automate everyday tasks in ESXi. It is also possible to connect vSphere ESXi nodes to an Active Directory domain, which eliminates the need to create local user accounts on each node.

Microsoft Hyper-V is a hypervisor-based hardware virtualization system. The logical unit of isolation supported by this hypervisor is the partition. Each instance of the hypervisor contains one parent partition running Windows Server 2008. A virtualization stack is run on the parent partition, which has direct access to hardware devices; this partition also spawns child partitions, where guest OSs are located.
Child partitions do not have access to hardware resources — they have a virtual resource view called virtual devices. All calls to virtual devices are performed through VMBus, a logical channel that provides communication between partitions, and are redirected to the devices of the parent partition to access the physical devices. Further, after starting VSP (Virtualization Service Provider) by parent partitions and its connection with VMBus, requests for child partitions are processed. Requests to the VSP of the parent partition are redirected through VMBus by the VSC client (Virtualization Service Client). Virtual devices also support Enlightened I/O, which allows to run directly with VMBus, which makes it possible to parallel processing of any layer of device emulation.

OpenVZ is an implementation of virtualization technology at the OS level and is based on the Linux kernel, as a result of which only Linux distributions can act as guest operating systems. This technology allows to run many isolated copies of the OS, called Virtual Environments (VE) or Virtual Private Servers (VPS). Each virtual environment contains its own files, users, groups, process trees, networks, devices, and IPC objects (inter-process communication). OpenVZ resource management consists of three components: two-level disk quota, fair CPU scheduler, and set of counters, restrictions and guarantees for each VE, called "User Beancounters". During virtual environments, resources can be changed without requiring a reboot. Distinctive features of OpenVZ are scalability, density and the ability to mass control VE.

Kernel-based Virtual Machine (KVM) is a virtualization tool in a Linux environment with support for hardware virtualization based on IntelVT or AMD SVM. KVM software includes a loadable kernel module to provide the core virtualization service, a processor-specific loadable module kvm-amd.ko (kvm-intel.ko), and user-mode components. The main concept behind KVM is to use the Linux kernel as a hypervisor. The /dev/kvm device is exported by the kernel module and makes its guest mode possible. Each virtual machine (VM) has its own address space, separate from other VMs and from the address space of the kernel, and its own virtual software. I/o operations from the guest operating system are performed by the QEMU platform to emulate hardware (disks, graphics cards, network devices, etc.). Any guest OS I/O requests are redirected to user mode for emulation through the QEMU process. Resource management in KVM is carried out using the Linux kernel mechanism of CGroups (Control Group).

8.3. Practical task

The customer's requirement is to transfer the server segment of the corporate ICT sector to dedicated servers of the data center using virtualization technologies. Develop a project to migrate server solutions and protect information resources of the virtual infrastructure (using the example of hypervisor or paravirtualized solution).

It is necessary to conduct a detailed benchmark analysis of existing virtualization solutions. Identify and eliminate existing vulnerabilities of the selected object. Design a corporate computer network (Intranet) with layers of protection. It is recommended not to forget about securing the administration, backup, live host migration and load balancing tools, as well as setting up virtual switches and routers. At the same time, it is necessary to consider the feasibility of using intelligent functions of network nodes (port security, IP-binding, ACL, VLAN, SNMP, etc.).

Report content

1. Purpose of work.
2. Statement of work.
4. Examining the selected hypervisor/paravirtualizer.
5. Design of architecture and security systems.
6. Finding and fixing vulnerabilities.
7. Conclusion.
8. References.
8.4. Control questions

Check yourself

What is software virtualization?
What is hardware virtualization?
What is paravirtualization?
Give the fundamental differences between discussed technologies. What are their advantages and disadvantages?
What is the purpose of the hypervisor?
Describe the working principle of ESXi, MS Hyper-V, OpenVZ, KVM systems. What are their differences?
What vulnerabilities do these virtualization tools have?
Give a benchmark analysis of these systems with tools not mentioned above.
9. Anonymization on the internet

Keywords: Proxy, secure channel technologies, VPN, Tor, I2P, TAILS, Kali Linux, Internet Surfing.

This chapter is devoted to technologies of anonymization and protection of data transmission on the Internet. Proxying mechanisms, as well as various implementations of technologies of virtual secure communication channels and overlay networks are considered.

9.1. Proxying mechanisms

If the purpose is to save network traffic (through compression, caching, etc.) and restrict user access, it is possible to consider proxying mechanisms. Proxy servers accept requests from users and execute requests to various network services on their behalf, which allows to hide the location of the sending host.

This technology can be used for various purposes:
1) saving network traffic through compression — data from the Internet is downloaded by a proxy server and transmitted to the user in a compressed form;
2) data caching — in case of frequent access to any external resources it is reasonable to store a copy of them on a proxy server, issuing data on request. Thus, the client receives the requested information faster, and the load on the communication channel to the external network reduces;
3) restriction of user access — restriction on the use of the Internet by specific users, ban on access to any websites, ads filtering, setting a quota for network traffic, etc.;
4) restriction of access to the local network from the outside — a possible option for configure a proxy server is the case when local nodes access external ones only through proxy server, while external ones cannot access local ones at all;
5) anonymization — a proxy server is able to hide or distort information about the sending node, then the target server can only access data about the proxy itself.

According to the principle of data transmission, there are two types of proxy servers: transparent and non-transparent. Their differences are due to the modification of messages transmitted through a proxy. A transparent proxy server can make changes to a request or response only if necessary. For example, it can add identification information about itself or the sender of the message. Moreover, it is obliged to ensure constancy of the Content-Length header value of the transmitted message. A non-transparent proxy server is capable of modifying the request and/or response: hide client data, convert format to reduce response size, translate text document, etc.

Both transparent and non-transparent proxies can have a cache associated with them. Also, both types of proxy servers play the role of an intermediate link between the web client and the web server, exchanging messages in the HTTP format (HyperText Transfer Protocol) (Fig. 8):
Proxy servers are divided into several types of functionality:

1) **HTTP/HTTPS** proxies are the most popular type of proxies. Depending on the level of anonymity provided, they are divided into the following categories: transparent — not hiding the true IP address of the client; anonymous — indicating the use of a proxy, but not showing the true IP address of the client; distorting — modifying the IP address of the client; elite — do not indicate the use of a proxy and hide the IP address of the client;

2) **SOCKS** proxy transmits data from the client to the server without making any changes to them. SOCKS proxy is a client for the web server. The most current version of the protocol is **SOCKS 5**;

3) **FTP** proxy is designed to upload data to file servers;

4) **CGI** proxies allow to surf the web anonymously. This type of proxy server does not require changing client settings.

The following sub chapters of the manual describe overlay network projects that use proxies.

### 9.2. Technologies of virtual secure communication channels

Next, it is necessary to consider the technology of the secure channel, whose task is to ensure the security of data transmission over an open transport network. The most common use case is on the Internet built on the TCP/IP protocol stack. Thus, in packet-switched networks virtual switching of secure channels is established, which includes the performance of three main functions:

1) mutual authentication of subscribers;

2) protection of messages transmitted through the channel from unauthorized access;

3) confirmation of the integrity of incoming messages on the channel.

An important characteristic of secure channel standards is the layer of the TCP/IP stack model on which these protocols operate:

1) Application layer — S/MIME / PGP / HTTPS and others;

2) Transport layer — SSL / TLS / SOCKS and others;

3) Internet layer — IPSec (AH, ESP) and others;
4) **Link layer — PPTP / L2TP / PAP/ MS-CHAP** and others.

**Virtual Private Network** called the connection of secure communication channels. These technologies allow you to deploy a logical network on top of the an existing one. Depending on the level of trust in the underlying environment, virtual private networks (VPNs) are divided into secure, created inside untrusted networks (**IPsec**, **OpenVPN** and **PPTP**), and trusted, used when the core network is considered secure (**L2P + IPsec**).

The most well-known implementations of virtual private network technologies are **IPsec (IP Security)** and **OpenVPN** protocols. **IPsec** has two modes of operation: transport mode and tunnel mode. In tunnel mode, the entire **IP** packet is encrypted, whereas only its contents are encrypted in transport mode, and the connection between the nodes can be formed using other technologies (**L2P**, etc.). The **OpenVPN** protocol uses the **OpenSSL** library to ensure the security of the transmitted data and have a lower-level of cryptographic security than **IPsec**. However, it is preferable due to its more correct operation in the presence of **NAT**.

There is a wide range of vulnerabilities in the algorithms of these protocols (due to the "rigid" logic of behavior) and their hardware and software implementation. Vulnerabilities are generally reviewed at least one year later. For example, the **OpenSSL** vulnerability **Heartbeat** and **MITM** were published on thematic resources of hackers on the **I2P** hidden overlay Internet network in 2012, and the official release of the security bulletins **CVE-2014-0160** and **CVE-2014-0224** was held only in April and June 2014, respectively.

It should be noted that with the correct configuration and further support by a technical specialist, this technology provides a reliable level of information security.

### 9.3. JAP Project

One of the key trends in the development of **ICT** is the research and development of **Overlay Networks**. This term refers to the organization of a logical network that operates on top of the Internet.

Highly specialized anonymous networks are the simplest type of overlay networks. As an example, consider the **JAP (Java Anonymous Proxy)** project. Its purpose is to anonymize the operation of the **HyperText Transfer Protocol (HTTP)**, i.e. web traffic.

The method of mix node traffic management shown in Fig. 9. The client sends data not to the desired destination, but to the host of cascades of mix servers that multiplex the information streams of different clients and send requests to their real destinations. Responses are broadcast along the same route. Client-server communication is carried out in encrypted form without the ability to adjust the chain of servers.

**Fig. 9. The method of mix node traffic management**

Compared to fully distributed systems, this method has the advantage of a higher speed of Internet Surfing (this term means visiting websites, searching and working with information on the Internet). At the same time, the client node does not act as the final link in the chain, i.e. on client's behalf the attacker will not be able to act within this network.

### 9.4. Tor overlay network

Acquaintance with the Deep Web should begin with a traffic management method based on **The Onion Router (Tor)**. A proxy server system is used to establish an anonymous network connection
ANONYMIZATION ON THE INTERNET

(illustrated in Fig. 10). The client randomly selects three proxy servers (nodes), exchanges encryption keys with them, and before sending information to the network produces multiple encryption (from 3 to 1 key) of each packet. Intermediate nodes can only decrypt their layer, having received from the useful information only the address of the next relay.

Fig. 10. The method of The Onion Router traffic management

Therefore, the intermediate nodes process the trace instructions and do not know the address of the sender and receiver, as well as the contents of the message.

9.5. I2P Project

No less meaningful development is the Invisible Internet Project (I2P). It is a secure anonymous self-organizing distributed overlay network. It has its own protocol stack, working on top of the TCP/IP model. The network provides a transport mechanism for applications to forward messages anonymously and securely. A modified DHT Kademlia with storage of hashed network host addresses, encrypted AES IP addresses, ND and public encryption keys is used. The technology deserves thorough consideration at all layers. But for the sake of brevity, it is necessary to give only the key concept of the method of the I2P traffic management, based on combined tunnelling (Fig. 11). Inbound tunnels are designed to send datagrams from the tunnel creator, and outbound tunnels are responsible for delivering datagrams to the tunnel creator. The chain is one-sided.

Fig. 11. The method of the I2P traffic management, tunnelling

By combining the two tunnels, node A and node B can exchange messages. Sender A sets up the outbound tunnel, and receiver B sets up the inbound tunnel. The inbound tunnel gateway can receive messages from any user and send messages to node B. The endpoint of the outbound tunnel is required to send a message to the inbound gateway. To do this, node A adds instructions to its encrypted message. Accordingly, when the datagram is decrypted at the endpoint of the outbound tunnel, instructions of
forwarding the message to the appropriate inbound gateway of node B are retrieved.

I2P uses a distributed network database to store and share network metadata, divided into two categories: routerInfo and leaseSets signed by one of the partners and verified by the opponent. The former ones provide information to border nodes to communicate with a particular router (public keys, transport addresses, etc.). The latter provide routers with data to communicate with particular objects of the destination nodes. The leaseSet parameters identify the tunnel gateway that allows to reach the destination node. To minimize the risks of unauthorized disclosure of the partner name in the network, another layer of encryption between the end nodes is added [60-64].

### 9.6. Tails operating system

*Tails* (The Amnesic Incognito Live System) is an operating system designed to anonymize users and ensure privacy. *Tails*, as is *Kali Linux*, is based on *Linux Debian*, but *Tails* can be installed as a replacement for the main distribution. This OS provides a wide range of mechanisms for ensuring anonymity, for example, after a system reboot all user actions are erased automatically. This does not make it possible to establish what kind of activity user conducted, and the contents of the clipboard are encrypted with the built-in system tools to hide it.

List the most well-known software for security and anonymity in *Tails*:

1) *Tor* with *Vidalia* Graphical User Interface (GUI) and *Torbutton* component to provide protection against malicious JavaScript codes;
2) distributed anonymous I2P network;
3) *HTTPS Everywhere* browser extension, which allows to access websites only using the https protocol;
4) *Pidgin* module for secure instant messaging in conjunction with the *OTR* (Off-The-Record) extension. It should be noted that dialogs are archived by default, so this option should be deactivated;
5) *GnuPG* program for data encryption and creation of electronic digital signatures;
6) *TrueCrypt* encryption program;
7) strong password generator *PWGen*;
8) *MAT* metadata anonymization tool (creation date, GPS coordinates, camera model, image creation options, etc.);
9) *Florence* virtual keyboard, which allows to prevent tracking of input data using keyloggers.

However, it is still worth noting that all the projects considered, including *Tails*, are not without vulnerabilities, which should be identified during the implementation of the practical task.

### 9.7. Practical task

You need to study the technologies of anonymization and protection of data transmission on the Internet. Then identify the vulnerabilities of the algorithms and working methods of the technologies considered, as well as the weaknesses of their software implementation.

The next step is to explore the tools of Internet Surfing. Conduct a benchmark analysis of browsers and their add-ons. Create a comprehensive software package for secure and anonymous work with information on the Internet. At the same time, do not forget to check your protection by specialized programs and services (for example, *WITCH* and *2ip.ru*).

Report content

1. Purpose of work.
2. Statement of work.
3. Research of technologies of anonymization and ensuring confidentiality of transmitted data.
5. Research and selection of Internet Surfing tools.
6. Conclusion.
7. References.
## 9.8. Control questions

**Check yourself**

- What are the methods of anonymization on the Internet?
- What are the main differences between the implementation of virtual private network technologies OpenVPN and IPsec?
- What are the proxying mechanisms? What are they used for?
- What networks are called overlays?
- What are the basic principles of the JAP network?
- What are the basic principles of the Tor network?
- What are the basic principles of the I2P network?
- What are the key differences between reviewed overlay networks?
- List the vulnerabilities of the reviewed projects.
- What is Tails OS? What features does it have?
Finding and exploring zero-day vulnerabilities

Keywords: Oday, back doors, Tor, I2P.

This chapter is devoted to the acquisition of skills of independent search, processing and analysis of information on the Deep Web. Actual software vulnerabilities and tools of hidden computer control are considered.

10.1. Theoretical information

A zero-day vulnerability (zero day, 0day) is the term for unresolved software vulnerabilities. The problem can be caused by both programming errors and inaccuracy of the algorithms and methods of the object functioning.

This vulnerability or attack becomes well-known until the software manufacturer releases bug fixes (updates, patches). Accordingly, it is impossible to detect such attacks with traditional signature defences. One of the possible solutions to the problem is the use of defences based on behavioral and intellectual-adaptive methods of information security.

The most critical vulnerabilities are hidden computer control tools called backdoors. This threatens privacy, and also there is a potential danger of malicious acts on behalf of someone else (impersonation attacks). Unfortunately, it is worth noting that software manufacturers themselves often integrate backdoors into their products, guided by commercial or political goals.

10.2. Practical task

You need to search and study zero-day vulnerabilities not previously published on the Internet, including on the manufacturer’s official website, and xakep.ru and habrahabr.ru resources.

You are required to demonstrate the skills of searching, processing and analyzing information on the Deep Web. It is recommended to use Tor and I2P hidden technical information resources.

An alternative way to complete the task is to independently analyze and identify vulnerabilities/backdoors of any software product.

Report content

1. Purpose of work.
2. Statement of work.
4. Analysis of the found zero-day vulnerabilities.
5. Research and development of defenses.
6. Conclusion.
7. References.
8. Listing.
10.3. Control questions

Check yourself

- What is called a zero-day vulnerability?
- What could be the cause of such vulnerabilities?
- What are the ways to detect attacks that exploit this vulnerability?
- Define the concept of backdoor.
- List the properties of backdoors.
- How can one identify zero-day vulnerabilities and backdoors in software products?
- Why is it recommended to use Tor and I2P hidden technical information resources to search for previously unpublished vulnerabilities?
An automated system of network and system administration of windows and Linux family operating systems

Keywords: system and network administration, user and server operating systems, Linux, Windows, ITSM, HelpDesk, ServiceDesk, primary identification of suspicious activity.

This chapter is devoted to the issues of automation of system and network administration of distributed information systems and corporate computer networks.

Automation of technological and business processes of an enterprise is one of the key trends in the development of information and communication technologies. Government agencies and commercial establishments design and implement corporate computer networks based on the TCP/IP protocol stack and Ethernet data link layer technology. The system and network administration of an organization’s information infrastructure is not only a creative engineering task, but also an important tool for optimizing an enterprise’s business processes. Accordingly, it significantly influences the economic performance of the company, as well as the level of its competitiveness in the market. In the early nineties, the scientific community developed a unified approach to the management of information technology as a service, which should have an appropriate quality and ensure a consistently high level of user satisfaction. This methodology was described in the IT Infrastructure Library. In May 2007, its third edition was introduced, describing the new format of the services’ lifecycle. Based on this library, a method of managing and organizing information technology services ITSM (IT Service Management) was developed, the key element of which were the user support systems: HelpDesk and ServiceDesk. The task of the first system was the accounting and management of user requests [65-67]. Originally, the technical requests of the company's employees were being processed by the information technology department. Systems like ServiceDesk were a logical extension of the HelpDesk systems, expanding their functions of managing incidents and service requests in all areas of the company’s activities [68]. In these systems, the functionality of providing feedback to users via various communication channels is implemented: e-mail, chat rooms, messengers, social networks etc. This enabled to form a service-oriented service, which is a single point of interaction between the service provider and the user [69-71].

Under this topic, a lot of research and development work is carried out by Russian and foreign scientists: Zabotina N.N., Zolnikova S.N., Sokolov N.E., Tipikin Yu.A., Odintsov I.V., Makhnovsky A. and many others [72-83].

It is worth noting that most of the proposed algorithms and methods allow to improve the quality of customer service and profitability of economic activity. However, these solutions do not consider the vulnerabilities of the TCP/IP protocol stack and software imperfections, including operating systems. Business interests lower the priority of high-quality technical implementation, which often complicates the activities of information technology departments, loading them with routine work.

Information security issues are an integral part of the task of automating technological and business processes of an enterprise. Potential damage caused by breach of confidentiality of commercial data may cause irreparable economic harm to the company.
11.1. Problem statement

The aim of the work was to develop and study an automated system of network and system administration of the Windows and Linux family operating systems, including the functionality of the HelpDesk and ServiceDesk solutions.

An algorithm for checking third-party software solutions for suspicious malicious activity needed to be developed and included in the system. In this context particular importance was given to the potential absence of antiviral agents on the client side. It was necessary to ensure both the security of network communications and the confidentiality of data on the client side.

11.2. Design and implementation of the system

The development and software implementation of the proposed network and system administration system of the Windows and Linux family operating systems was carried out in two versions. The first version was presented as an independent end product, commissioned by a commercial holding. The second version was designed and implemented as a module of the system of intellectual and adaptive management of the enterprise’s network infrastructure developed by the author.

This article presents the material of the second project implementation. At the design stage, the following functions of the developed system were embedded:

- receiving and processing requests through various communication channels (e-mail, online chat rooms, messengers, social networks, etc.), primary communication with customers or employees of the company;
- semantic analysis of the query text, an attempt to automatically solve the problem or provide a suitable article from the knowledge base;
- evaluation of the request, delegation to the most appropriate specialist in the absence of the possibility of applying the solution in automatic mode;
- accounting and tracking of requests and incidents;
- informing customers/employees about the status of requests and the progress of their execution;
- monitoring the level of service in accordance with the SLA (Service Level Agreement);
- management of the lifecycle of incidents and requests, including their closure and verification;
- alerting, informing and coordinating employees and customers;
- providing tools of a flexible project maintenance methodology;
- processing and analysis of logs of the operating system and installed software in the enterprise corporate computer network;
- providing tools to verify third-party software solutions for suspicious malicious activity in corporate computer network;
- automatic identification and solution of local technical problems;
- monitoring network infrastructure of the enterprise;
- monitoring employee activity on personal computers;
- and many others.

The proposed original solutions in the field of system and network administration are worth considering in more detail. At first sight, processing and analyzing the logs of the operating system and the installed software is a rather trivial task. However, a simple example of the remote work of the user of host A on host B for one hour using the Remote Desktop Protocol (RDP) should be given. In the event log of the Windows operating system EVTX (XML EventLog) there may appear more than 60 entries of entry/exit events with identical id instead of the expected two.

Another interesting example is the work with the volume shadow copy service, which can be accessed by various applications and services, including over the network. If this service fails, the number of events per minute can exceed 500 units, cyclically referring to each other. To compile an objective picture of what happened, it is necessary to collect additional information from the system, parse, process and analyze it. In order to meet such objectives, an enhanced signature approach with the identification of event
correlation was integrated with the system. The initial knowledge base was compiled in a virtualization environment based on the ESXi hypervisor, which had more than 10 copies of each of the popular Windows and Linux family operating systems being deployed. Next, the tools of testing, passive and active analysis of operating systems and applications were used. For local testing, additional scripts which caused failures and malfunctions were written to check the reliability and fault tolerance of the software. During one hundred iterations of each individual network/local disturbance, the client-server model tracked the events being recorded and identified the correlation. Thus, the initial knowledge base was being compiled.

Importantly, each iteration was carried out towards the reference image of the operating system, a return to which was driven through snapshots system. Adding new entries to the general knowledge base of the corporate solution is being carried out only on the basis of similar results from 50% of clients with the number of hosts with identical software from 10 units.

This approach allowed to perform the automatic identification and solution of local technical problems. The situation with the problem of the receipt of the TCP/IP protocol stack settings by the host can serve as a simple example. The system identifies the failure of the DHCP-client service, tracks its dependencies on other services and finds the one being stopped. After that the system launches them in the correct order and restoring the full functioning of the service.

To implement the verification of third-party software solutions for suspicious malicious activity, an original algorithm was developed, shown in Fig. 12.

This algorithm provides the technician and/or technically competent user with a qualitative analysis of the object being investigated: whether functions undeclared by the developer are present, whether any information is being sent to third parties, etc. However, it is important to note that the algorithm does not replace a full-fledged audit of the program code (including that being carried out through disassembly). It is also not possible to detect in a closed source code a tool for hidden data collection or information management (backdoor), if it was in passive (“sleeping”) mode.

Monitoring of the enterprise network infrastructure is being carried out using network management protocols and a decentralized knowledge base of participants in the interaction of the corporate computer network. This includes control of the versions of the installed software and the hardware solutions used on each device. This functionality is fully implemented by the system of intellectual adaptive management of the enterprise network infrastructure, developed by the author. As noted previously, the network and system administration system of the Windows and Linux family operating systems is its integral part. The components of the client part of the system are illustrated in Fig. 13.
AN AUTOMATED SYSTEM OF NETWORK AND SYSTEM ADMINISTRATION OF WINDOWS AND LINUX FAMILY OPERATING SYSTEMS

![Flowchart diagram](image)

**Fig. 12. Algorithm for checking third-party software solutions for suspicious malicious activity**
The decision to use different components in the same client software implementation was made taking into account two factors. The first is the necessity of ensuring the comprehensive intelligent adaptive management of the enterprise network infrastructure. The second is the willingness to optimize the use of the computational power pool, since most components have overlapping functionality and access to the same resources. It is firstly referred to the operating system and application logs, however, in some cases, to the access to equipment. Thus, the system of intellectual control and management of access to information resources of a personal computer controls the connected data storage devices and used data transmission networks. The purpose of these actions is to prevent illegal copying of information. At the same time, an automated network and system administration system monitors the operation of hardware resources in order to provide reliable and fault-tolerant functioning of the host.

During the work, the architecture of the server part of the system was designed and implemented, as shown in Fig. 14.
The software solution was created using the platform for applications automated deployment and management in a virtualization environment. This ensures a high level of reliability and fault tolerance of the system.

The software implementation of the server part was performed using Python, Flask, C++, Bash, Docker, Ansible on the basis of AlpineLinux OS. The client module for Windows family operating systems was written in the C# programming language using native controls from the Windows Forms .NET library. For the Linux family, Python and the Qt framework were used. Encapsulated virtual secure communication channels (VPN, Virtual Private Network) helped to ensure the protection of data transmission over the network. Depending on the project build, the following technologies were used: GateVPN, GoVPN, Tinc, WireGuard, FreeLAN, OpenVPN, IPsec and others. Secure local data storage was provided by the symmetric block encryption algorithm AES-256 (Advanced Encryption Standard).
Both during the development and afterwards, manual and automated testing of the developed software product (client and server parts, as well as their interaction) was performed.

The developed solution significantly extends the existing systems such as HelpDesk and ServiceDesk. The integration of the first version of the system at the customer’s enterprise (with a number of hosts of more than 500 units) allowed to optimize the work of the information technology department and to reduce the time costs for system and network administration of the existing infrastructure of the company by 70%. The general knowledge base of the system is not updated in enterprises with fewer than ten hosts, which may be mentioned as a disadvantage of the proposed approach. Adding new entries to the general knowledge base of the corporate solution is carried out only on the basis of similar results from 50% of clients with the number of hosts with identical software from 10 units. The described development has been registered as an object of intellectual property [84].

11.3. The discussion of the results

In this tutorial the design and implementation of an automated network and system administration system for Windows and Linux family operating systems, which includes the HelpDesk and ServiceDesk solutions functionality, was presented. The signature method of the operation of the system with the identification of the correlation of events is reviewed. The original approach to creating a knowledge base of the system is described. The solution was implemented using a platform for automated deployment and management of applications in a virtualization environment, which provides an additional level of reliability and fault tolerance. An algorithm for checking third-party software solutions for suspicious malicious activity is proposed, providing a qualitative analysis of the object being investigated: whether functions undeclared by the developer are present, whether any information is being sent to third parties, etc. A comprehensive approach to the management of the enterprise network infrastructure is also reviewed. In order to ensure information security of network communications, encapsulated secure virtual communication channels were used, while AES-256 encryption algorithm was used to ensure data privacy on the client side.

The proposed approaches are recommended for use in enterprise network infrastructure management systems with a number of hosts from ten units operating on the basis of the TCP/IP protocol stack and the Windows/Linux family operating systems.

11.4. Practical task

You need to search and study the existing HelpDesk and ServiceDesk solutions, as well as tools for monitoring local and network information processes and flows. You need to conduct a benchmark analysis of selected software products with well-known solutions of system and network administration of distributed information systems and corporate computer networks.

Report content

1. Purpose of work.
2. Statement of work.
4. Analysis of the found zero-day vulnerabilities.
5. Research and development of defenses.
6. Conclusion.
7. References.
8. Listing.
11.5. Control questions

Check yourself

Describe the ITSM methodology.
How to identify suspicious software activity?
Describe the purpose of HelpDesk systems.
What are the differences between HelpDesk and ServiceDesk solutions?
List the methods of monitoring network infrastructure.
How can one automate the processes of system and network administration?
How is the security of the process of automating the collection, processing and information management ensured?
Conclusion

As part of this tutorial, we introduced the conceptual principles of system administration and integrated information security of distributed information systems and corporate computer networks. Theoretical material that helps to gain practical skills in designing networks, setting up and configuring software, managed hardware and software tools at the corporate level is presented. The work of the system administrator and information security engineer in the most common operating systems of Windows and Linux family is considered.

The operation of gateways, web servers, file servers, firewalls for protecting web applications (WAF), and intrusion detection and prevention systems (IDS/IPS) is analyzed. Basic skills in the basics of administering centralized user work and knowledge in virtualization technologies were acquired. Vulnerabilities of the computer network traffic management are systematized, an overview of solutions to the issues of anonymization and secure Internet Surfing is given. Partially, cryptography and the practical side of privacy were affected both on the local-side and in the network interaction.

The authors sincerely hope that the reader was able to develop skills in search, processing, systematization and analysis of information. Because in life, it is necessary to be able to make balanced, constructive and reasoned decisions, study the material at a conceptual level and quickly solve the tasks in the shortest possible time. Now the thesis about the impossibility of achieving an impeccable level of information security should be perceived constructively. It is necessary to find a compromise in terms of cost-effectiveness and expediency.

This tutorial is the result of the fruitful and efficient work of the Novosibirsk State Technical University under the program called "SMARTCITY: Innovative Approach Towards a Master Program on Smart Cities Technologies" (which lasted from 15 November 2018 to 14 November 2021). Its guideline is the creation of a new generation of interdisciplinary engineers of information and communication technologies in the field of Smart Cities. The project complies with the principles of the Bologna process and aims to develop the European Higher Education Area.

Bearing in mind international trends in the field of political censorship and total control, one should not forget that the invention of various algorithms and methods of information security and anonymization, the development of innovative IT solutions and the publication of them with open source code are beneficial to society.
References


10. The Onion Router. Available at: https://www.torproject.org (accessed 31.08.2015).


42. Basinya E.A. Voprosy upravleniya trafikom v overleinykh setyakh [Issues of Traffic Management inOverlay Networks], Avtomatika i programmnya inzheneriya = Automatics & Software Enginry, 2014, no. 3 (9), pp. 29-32. (In Russian)


47. Basinya E.A. Problematika upravleniya trafikom vychislitel'noi seti s kommutatsiei paketov na osnove steka protokolov TCP/IP [The Problems of Traffic Management of a Packet-Switched Computer Network Based on The TCP/IP protocol stack], Teknika i tekhnologiya: novye perspektivy razvitiya [Engineering and technology: new development prospects], 2014, no. 15, pp. 48-57. Rabota vypolnena pri finsosvoi podderzhke Minobrnauki Rossii po gosudarstvennomu zadaniu №2014/138 tema proekta «Novye struktury, modeli i algoritmy dlya proryvnykh metodov upravleniya tekhnicheskimi sistemami na osnove naukoemkih rezul'tatov intellektual'noi deyatel'nosti» [This work was financially supported by the Ministry of Education and Science of the Russian Federation on state assignment No.2014/138 the theme of the project is "New structures, models and algorithms for..."].
breakthrough methods of managing technical systems based on knowledge-intensive results of intellectual activity”] (In Russian)


70. Sterlyagov S. P., Bezymanych N. A. Sovershenstovanie deyatelnosti otdela informatsionnykh tekhnoLOGii nalogovoj inspektsii na osnove metodologii ITSM/ITIL [Improving the activities of the information technology department of the tax inspection based on the ITSM/ITIL methodology]. Internet-zhurnal naukovedenie [Online journal science research], 2017, vol. 3, no. 3. 105 p. (In Russian)


72. Zabotina N.N., Vasil'kovich Yu.V., Gushchina L.S. Upravlenie incidentami v IT-infrastruktury predpriyatiya [Incident management in the enterprise IT infrastructure]. Informatizaciya i svyaz' [Informatization and communication], 2016, no. 2, pp. 31-35. (In Russian)

73. Malaev A. N. Kachestvo operativnogo upravleniya v sfere tekhnicheskoy podderzhki bankovskikh ustroystv samoobsluzhivaniya [Quality of operational management in the field of technical support of self-service banking devices]. Izvestiya orenburgskogo gosudarstvennogo agrarnogo universiteta [Izvestia, Orenburg State Agrarian University], 2015, no. 1 (51), pp. 223-225. (In Russian)

74. Zol'nikova S.N., Deberdieva E.M. Povyshenie effektivnosti deyatelnosti IT-podrazdeleniya [Improving the efficiency of the IT department]. Ekonomika i predprimatelnstvo [Economy and entrepreneurship], 2014, no. 11-3 (52), pp. 364-368. (In Russian)


76. Sergeeva A. Raspredelennye virtual'nye stendy dlya testirovaniya veb-servernykh prilozhenij [Distributed virtual stands for testing web server applications]. Sistemnyj administrator [System Administrator], 2014, no. 11 (144), pp. 78-84. (In Russian)


78. Ponachugin A.V., Odincov I.V. Sistema kontrolya za nesankcionirovannoy deyatelnost'yu pol'zovatelej komp'yuternoy seti [Control system for unauthorized activity of computer network users]. Programmnaya sistemy i vychislitel'nye metody [Software systems and computational methods], 2016, no. 1, pp. 23-31. (In Russian)


80. Efremova L.I., Kurganov A.N. Formirovanie portfelya prilozhnykh sistem dlya predpriyatiya gazodobyvayushchej otрасли [Formation of a portfolio of application systems for the gas industry]. Informatsionnye sistemy i tehnologii [Information systems and technologies], 2017, no. 3 (101), pp. 57-66. (In Russian)

81. Filippov O. Instrumenty tekhnicheskoy podderzhki filial'noy seti [Branch network technical support tools]. Sistemnyj administrator [System Administrator], 2017, no. 4 (173), pp. 34-37. (In Russian)


84. Basinya E.A. Avtomatizirovannaya sistema setevogo i sistemnogo administrirovaniya operacionn'x sistem semeistva Windows i Linux [Automated system of network and system administration of Windows and Linux family operating systems]. Patent RF, no. 2018662438, 08.10.2018. (In Russian)