ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 7, Issue 7 , July 2020

Analysis of Attacks and Information Security Violations in Information-Computer Networks

Turaev Bakhtiyor Temirovich

Teacher of the department "Management of the daily activities of the troops"
Academy of the Armed Forces of the Republic of Uzbekistan

ABSTRACT: The article presents the causes and sources of information security violations, the main types of computer attacks on military information networks, as well as the classification of computer attacks according to their characteristics.

KEY WORDS: information, attacker, computer attacks, military computing networks, network scanning, password attack, denial of service.

I. INTRODUCTION

Rapidly developing and improving information technologies bring significant changes in all aspects of our daily lives. Currently, the concept of “information” is used as a special trademark that can be bought, sold, exchanged for another tangible item. In most cases, the cost of information is several thousand times higher than the cost of telecommunication network equipment. This is one of the problems, and the main problem is the leak of any important information that could adversely affect the economic and social competence of the whole country, especially if such information is directly related to the state security of the country. Currently, one can observe a sharp increase in threats in information systems, including military information and computer networks.
Based on the foregoing, there is an urgent need to consider the urgent issue of applying measures to prevent malicious acts in a timely manner, such as disclosing, modifying, destroying or hiding information. To achieve the objectives, first of all, it is necessary to analyze the causes and sources of attacks that fall upon us like a storm.

II. SIGNIFICANCE OF THE SYSTEM

Everyone knows that in military control systems, the exchange of information between network elements, as well as the management of forces and means, is carried out through specially organized military information computer networks (further MICN or network) designed to achieve these goals.
To ensure a high degree of protection of information circulating in the MICN and to prevent potential threats to the network, it is necessary to identify the causes and sources of data security breaches.
To ensure the protection of the MICN, the following principles must be observed:
Firstly, the choice of network security tools, their installation, configuration, as well as the solution to the problem of restricting unauthorized actions in the data circulation process;
Secondly, constantly identify, search and track insecure network nodes from which data is output.
In MICN negative human actions have a significant impact on information security and these negative factors can be observed in descending order:

– viral attacks;
– terminal theft;
– insider actions;
– remote access.

It can be seen from the above procedure that the risk of threats to the information security of the MICN created by employees directly related to this system is higher than external threats. Therefore, the choice of staff for the network is one of the key elements of security.
Accidental or deliberate exposure of employees with administrator rights in the system can lead to serious problematic risks. Threats created by employees can be divided into three groups depending on the presence of malicious actions:

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 7, Issue 7 , July 2020

"Careless". An employee who doesn't understand the safety rules, despite the instructions, and as a result makes mistakes when working with data. Because it is so reliable and deceptive, it is easy to use with unauthorized access to illegal confidential information.
"The intruder." No one can consciously commit harmful acts without a clear reason. The reasons can be different - from physical interest to the indignation of the boss, especially the employees performing additional official duties in the interests of other interested parties [2].
"System Administrator". A loyal employee with super user rights, who performs deliberate actions that can cause harm in any situation. This may be due to a lack of basic skills, fatigue, overwork.
The following are the types of actions that can be taken to gain unauthorized access to information on networks:

- violation of confidentiality of information;
- using the authority of another user (to relieve oneself of responsibility) representing himself as a person authorized to receive unauthorized information, permission to enter false information into computer networks or confirmation of false information;
- refusal to organize access to information;
- the issuance of false information, indicating that it was organized by another network user;
- an indication that the information was sent to the recipient at the indicated time, or to falsify the time when the information was sent;
- denial of the fact that the data was received, or falsification of the actual time of receipt of the data;
- unauthorized extension of the authority of the information system provided to users in organizing, transmitting, disseminating information and in other areas;
- unauthorized change of user privileges;
- express important information as insignificant;
- unauthorized connection to network access points and regular distribution of information from it to other networks;
- analysis of the data flow in the network to study what data users receive;
- cast doubt on the protocols, violating the confidentiality of information;
- making changes to the data protection algorithm program using an inconspicuous procedure;
- carrying out actions that lead to a denial of the authenticity of the transmitted data, interfering with the quality of data transfer to other network users, in particular, invisible technical, software and other methods.

We know that no matter how strong the information protection systems in networks are, the number of those who are interested in breaking into this network will not decrease, but on the contrary, attacks will continue to improve.

III. LITERATURE SURVEY

Need of an attack analysis
The presence of vulnerabilities (vulnerabilities in the data processing system) in the MICN creates the conditions for threats to information or information resources, and with the help of these vulnerabilities an attacker gains the ability to conduct targeted computer attacks.
Computer attacks (hereinafter referred to as an attack) are understood as an attempt to violate computer security by an attacker, unauthorized access to information systems, gaining control of the system and its elements, or disrupting their operation, or refusing to service various services, as well as deliberate potential actions leading to to violation of confidentiality, integrity, accessibility and safety of information circulating in the MICN. A computer attack is carried out in the form of a specific target (malicious) program or sequence of commands.
The MICN differs from other networks in that important information circulates in it. They use various expert information security systems, information security monitoring systems and attack detection systems. Ensuring fast, uninterrupted, and covert command and control of troops requires, first of all, rapid detection and elimination of attacks in the MICN, otherwise organized attacks can lead to failures in the performance of combat missions, data loss, false data entry, network instability or complete failure, which will lead to serious consequences.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 7, Issue 7 , July 2020

Therefore, all of the above factors are present and require the timely and effective application of measures necessary to counter possible attacks. To solve these problems, it is necessary to deeply study and analyze the most common modern computer attacks, their types, causes, sources, mechanisms of action and characteristics of their impact.

Attack classification

In 1996, the scientist Fred Cohen worked on the mathematical theory of viral technology and proved that the number of viruses is infinite, respectively, the number of attacks is also infinite. From this we can conclude that if the number of attacks is infinite, then the number of methods and means of organizing attacks will also be unknown, that is, attacks will differ in their variety. But the main purpose of carrying out all types of attacks is to gain access to other people's information, as well as inflicting certain moral and material damage /

Given the research conducted in this area and a number of factors, attacks can be divided into the following groups [1]:

– **in order to implement:**

- ***intelligence (data collection);***
- ***exploit (abuse);***
- ***denial of service.***

Attacks on MICN are organized mainly for the purpose of reconnaissance, full or partial control, or the destruction of information systems and can be carried out using various methods and tools.

Intelligence service. These attacks are carried out by attackers who do not have specific permissions in order to collect information about the network and their elements, in particular about the network architecture, detect its vulnerabilities (open ports), and analyze the flow of information circulating in it.

In fact, in a MICN this type of attack is aimed at peeping, listening and intercepting data, that is, violating data privacy, and is carried out in three different ways:

scanning the network and its vulnerabilities;

scanning network data transfer protocols;

traffic analysis.

Network scanning and its vulnerabilities are one of the most powerful tools and are conditionally divided into means for scanning IP addresses, ports and vulnerabilities.

IP address scan,attacks are carried out using the ICMP (Internet Control Message Protocol) protocol by sending packets of the ICMP ECHO type to the specified IP address and waiting for a response packet from it. If in this case the response packet is ICMP ECHO_REPLY, then the specified address is considered to be connected to the network. It is also possible to capture a lot of useful data when exchanging ICMP packets with arbitrary network addresses. Scanning tools: WS PingPro, Advanced IP Scanner, Advanced LAN Scanner, IP-Tools.

*Port scan*attacks are carried out by test connection to the TCP and UDP ports of the computer under investigation, in order to determine the running services and their corresponding ports. As a result of port scanning, an attacker can obtain information about the computer's operating system, as well as about the software running on it. For example, Advanced Port Scanner, Angry IP Scanner.

Vulnerability Scan carried out by an attacker in order to identify active IP addresses, open ports, running operating systems and applications on computers on the network, as well as the availability of identified vulnerabilities. For example, Nessus, GFI LANguard, Retina, X-scan, OpenVAS, Xspider, QualysGuard.

Traffic analysis attack It is carried out mainly with the purpose of listening to the communication channel, analysis of the transmitted data and related service information to study the architecture of the system, to obtain confidential user information. The target of an attack can be, for example, the internal network of a military unit, if this network goes online. It should be noted that traffic analysis is one of the main methods of electronic intelligence and electronic warfare. Traffic Analysis Tools: Wireshark

Thus, the likelihood of an attacker attacking a MICN by means of traffic analysis is very high.

Exploit (abuse).

These attacks are carried out locally or remotely in order to obtain full or partial control (or control) over the MICN and its elements, obtain passwords, unauthorized changes to security settings, violation of information integrity, as well as to reduce network performance.

In fact, in a MICN this type of attack is aimed at replacing, changing, deleting and hiding data, that is, violation of data integrity. In this case, the actions are performed by a computer program, fragments of program code or a sequence of commands, in short, by malicious programs (for example, logical bombs, Trojan horses, viruses or worms).

Password attacks. It is well known that in order to violate the security of a computer, network devices, as well as data security, attackers must first identify security vulnerabilities or cryptographic algorithms used to protect data. If an

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 7, Issue 7 , July 2020

attacker logs on as a user and has certain rights, then the security systems used to protect data, as well as cryptographic algorithms, may be useless. Based on this, we can conclude that the weakest points of automated information systems are access points to this system. In turn, these access points will be protected by authentication protocols (especially passwords and logins), which can make it difficult for an attacker to bypass the authentication system.

Password attacks can be divided into five groups (types): guessing, resetting, breaking, analyzing and capturing passwords. These actions can be performed locally or remotely, manually or automatically using a number of methods, such as exhaustive search, trojans, IP spoofing, packet capture methods (FTP packet), keylogging.

Password guessing. These types of attacks are carried out by an attacker using a number of methods, such as direct selection (dialing), character selection, or dictionary selection using password selection tools. Examples of such tools are John the Ripper, Hydra, TSGrinder, SQLRecon, Cowpatty.

Reset your password. This method is often used by an attacker to bypass the authentication mechanism when entering the system, as well as on locked computers and in cases where it is not possible to select passwords, mainly for canceling local administrator passwords in the local database. But an attacker prefers to find passwords and then log in, rather than reset passwords at logon. These tools include Winternals ERD Commander.

Password cracking. These attacks are carried out by an attacker using the method of extracting the hash value of passwords or other hidden forms of text passwords and converting them to the original version of the password based on the information received. Examples of such tools are Aircrack, RainbowCrack, Pwdump, John the Ripper, HashCat.

Password Analysis. This attack is carried out by an attacker using an authentication traffic analysis method to crack passwords by obtaining a password hash or enough information about them. Examples of such tools are Cain & Abel, ScoopLM, KerbCrack.

*Password capture.*Typically, these types of attacks are carried out by attackers using Trojan horses, as well as hardware and software that controls the keyboard. An example of this are keyboard recorders that are installed between the computer port and the keyboard cord.

Denial of service*(DoS - Denial of Service).*

Through these types of attacks, an attacker tries to perform actions such as shutting down information systems, including MICN and its elements, disabling the services provided by the system, filling disks with unnecessary data. As a result, users with authority in the information system are prohibited from using the data processing system and its resources.

In addition, these situations may not always be deliberate, and sometimes they may occur by accident due to errors in the information system and its elements.

In fact, attacks aimed at denial of service in the MICN are carried out locally and remotely and include four different types of attacks: denial of access to information, applications, the system, and telecommunication facilities.

Denial of access to information. These DoS attacks are carried out by an attacker by creating unsuitable information for use (in this case, the data will be destroyed, damaged or moved) in order to prevent authorized users of information systems from using the information that they present to them.

*Denial of access to the system.*These DoS attacks are aimed at shutting down a computer system, as well as other means of telecommunication. As a result, these tools and the data, applications stored in them, as well as all the services they provide, will be unavailable.

Denied access to applications. These DoS attacks are carried out in order to disable applications that process or describe data, or computer systems that run these applications.

Denial of access to telecommunications. These DoS attacks are carried out without compromising data integrity, but with the goal of disabling the telecommunications environment that enables the data exchange process. For example, MICN can be used as an example of data traffic overflow by distributing a large number of message packets (requests) or by suppressing radio signals when data is transmitted by radio.

Based on this, DoS attacks differ from other attacks in that they are not designed to gain unauthorized access to your network or change any data in it, but to make this network and its elements, as well as services unsuitable for use. If DoS attacks are organized from several devices at the same time, such attacks are called distributed DoS attacks (distributed DoS, DDoS).

Well-known DoS attacks: TCP SYN Flood, Ping of Death, Tribe Flood Network (TFN), Trinco, Stacheldracht, Trinity.

– **by the nature of the impact:**

- ***passive (inactive) attacks;***
- ***active (active) attacks.***

Passive attacks. These attacks are aimed at unauthorized collection and monitoring of information about networks and its users, as well as data transmitted over the network, without compromising the performance of information resources

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 7, Issue 7 , July 2020

on the network, which in some cases can violate its security settings. Passive attacks are mainly carried out for the purpose of reconnaissance, using the methods of listening and peeping (analysis of the data stream) of information resources, in particular, information circulating in the MICN.
Since passive attacks are not intended to violate data integrity, that is, there are almost no signs that passive attacks have occurred, they are very difficult to detect. Therefore, in ensuring information security in the network, the main attention should be paid to the prevention of passive attacks, and not to their detection.
Active attacks. These types of attacks are carried out with the aim of directly disrupting the operation of the information system, the security policy adopted in it, as well as their integrity by modifying the information circulating in the MICN. Most of these attacks can be carried out both remotely and locally.
In MICN there are three types of violations of the integrity of information: replacement, addition and deletion.

- **at the place of origin:**
- ***local attacks;***
- ***remote attacks.***

Local attacks. In a MICN, an attack is carried out when the object and subject of the attack are inside the same network segment, under conditions when the stations are physically connected to each other using communication devices not higher than the channel level. In addition, the subject of the attack can also be authorized users, network administrators, or malware belonging to the network.
Remote attacks. This type of attack is carried out by an attacker, remotely, mainly using software, in order to destroy the information resources of any other network that does not belong to its segment. Attacks such as network traffic analysis, replacement of authorized tools, and denial of service can be called remote attacks.
Thus, all computer attacks are carried out locally or remotely. However, the consequences of local and remote attacks can be almost the same, but there are some difficulties in identifying remote attacks, since the attack object will belong to another network and can be located at a distance of several thousand kilometers.

- **by the number of attackers:**
- ***unallocated attacks;***
- ***distributed attacks.***

Unallocated Attacks conducted by one attacking entity with respect to one (or more) attacking objects.

Distributed attacks- this is an attack on one (or several) objects of attack by two or more attackers, based on a carefully planned plan, mutually agreed on one idea and time. Basically, such attacks are based on a denial of service type of attack (for example, SYN-Flood, Smurf, UDP Flood, Targa3 and other attacks).

– **by the presence of feedback with the attacked object:**

- ***with feedback;***
- ***without feedback.***

With feedback. This type of attack is characterized by the ability that the subject of the attack receives responses to requests from the target of the attack. This means that feedback is formed between them, and as a result, the attacker constantly receives information about the situation with any change in information resources at the attacked object.
No feedback . Non-feedback attacks typically include one-way attacks. For this type of attack, information about changes in the information resources that are being attacked is practically irrelevant (for example, DoS attacks).
Thus, feedback attacks are more complex than feedbackless attacks, since they require active communication channels between the attacking subject and the object for continuous data transmission. Feedback attacks are considered more dangerous.

– **by nature of occurrence:**

- ***deliberate attacks;***
- ***random attacks.***

Intentional attacks. In a MICN, these attacks are carried out by an attacker or a group of persons on the basis of a clear plan, by order or of their own benefit, with the aim of unauthorized modification, destruction, access, disclosure or collection of data, without appropriate authority. Consequently, that intentional attacks are material and moral damage, that is, material (moral) damage to the target of the attack or material (moral) damage to the subject of the attack.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 7, Issue 7 , July 2020

Random attacks . In a MICN, these attacks can be random from unauthorized network users, network administrators, or due to a lack of knowledge on the use of information technologies, as well as errors and unstable operation of information system resources. Random attacks can also cause quite a lot of material and moral damage.

– **by the nature of the damage:**

- ***material;***
- ***moral.***

Attacks for material purposes. As far as we know, information is a special trademark, a product that reflects reality, in which case it can be bought, sold, exchanged for another tangible item. Therefore, in MICN these attacks can be carried out with the aim of causing material damage to someone or something, in particular the object of attack, or material benefit to the subject of the attack as a result of disclosure, modification, destruction or concealment of information.

Attacks for moral purposes. These attacks are carried out with the aim of causing moral harm to someone or something as a result of disclosure, alteration, destruction or concealment of information.

Thus, taking into account the specific features of military information and computer networks, as well as the above factors, computer attacks can be classified as follows.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 7, Issue 7 , July 2020

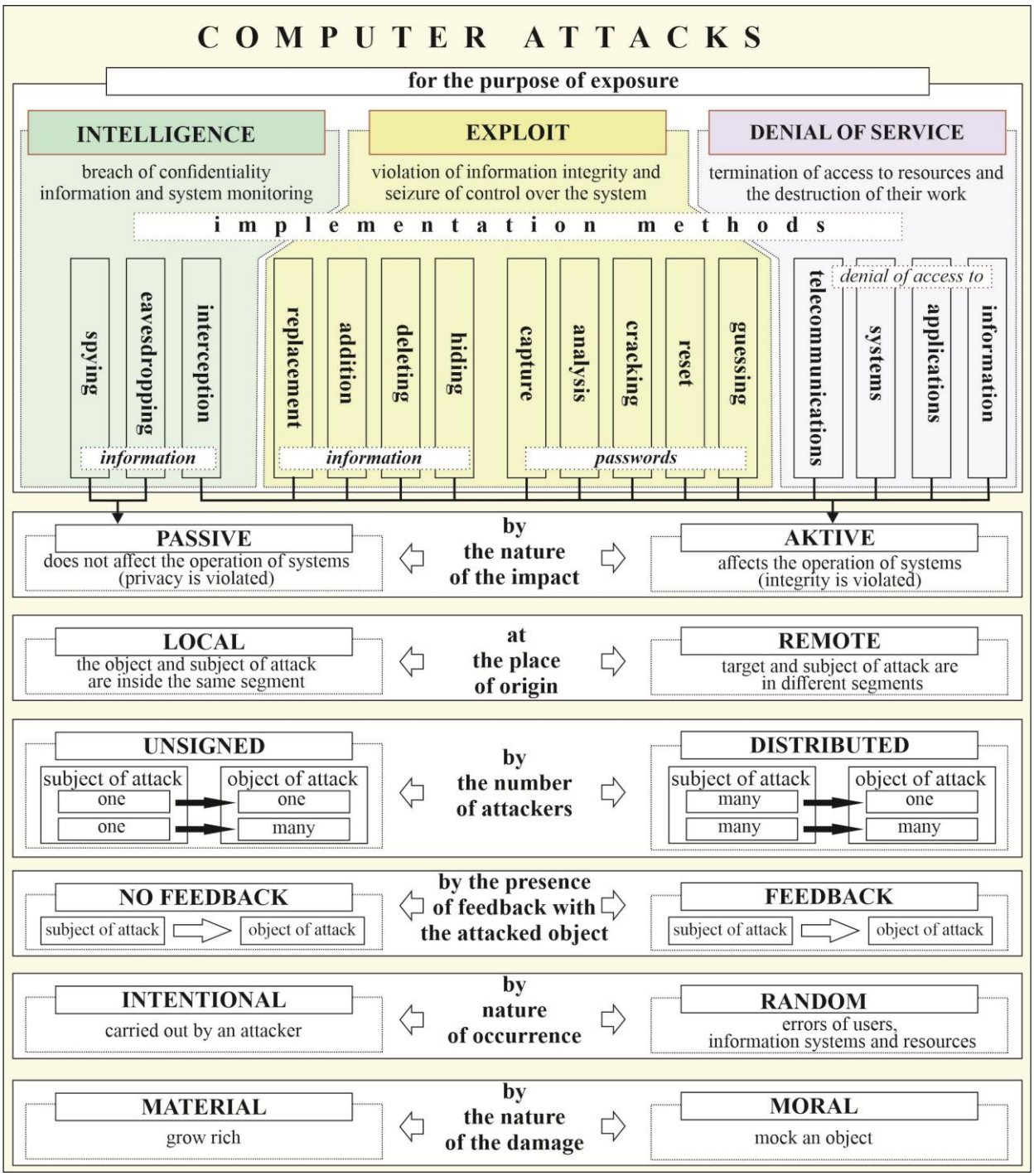

Figure 1. Classification of attacks.

Since it is known that each attack starts at a certain time and ends at a certain time, regardless of whether the goal is reached. In [5], it describes in detail the stages of an attack, that is, the implementation of the attack includes the following steps (Figure 2):

I. ***preliminary actions before the attack or data collection;***

II. ***the main stage of the attack or the implementation of the attack;***

III. ***attack completion.***

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 7, Issue 7 , July 2020

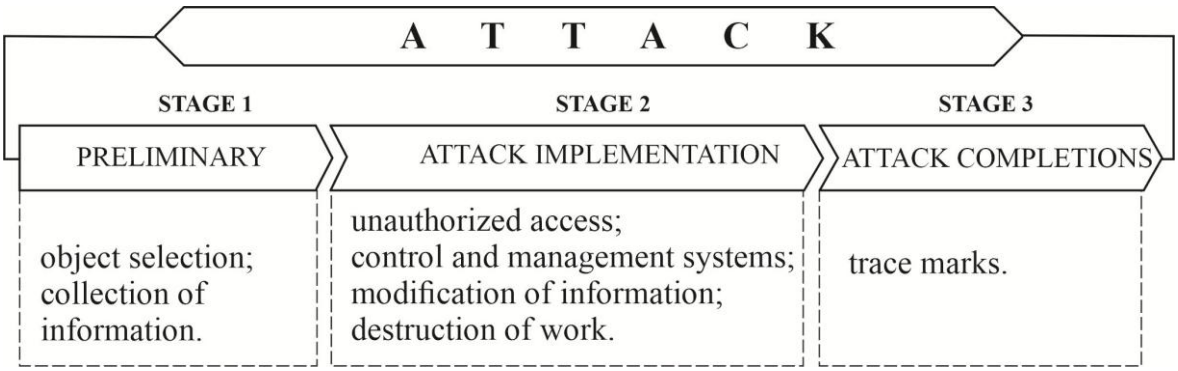

Figure 2. Stages of attack implementation.

At the first stage the attacker selects the attack target, determines the target of the attack and collects information about it, in particular, the type of operating system used in it, its open ports, running services, installed system and application software, and their configuration, security settings. Then he identifies the weaknesses of the object and creates the conditions for the implementation of the next step.

In the second stage the subject of the attack enters the target of the attack (without permission) and reaches the intended target of the attack. For example, actions such as taking control of a system, changing data, turning off system resources, etc.

At the last stage the attacker destroys the corresponding entries in the node's registration log and other actions that return the attacked system to its original, "pre-attacked" state.

As a result of such research, opportunities can be opened up to create the most advanced methods and tools effective in countering attacks.

IV. CONCLUSION

Thus, the presence of vulnerabilities in military information and computer networks creates the conditions for threats to information or information resources, and with the help of these vulnerabilities an attacker is able to carry out targeted computer attacks. In order to come up with "how to detect", you need to know "what to detect". It is important to understand the types of attacks and their classification.

REFERENCES

[1] Sheluksin O.I., Sakalema D.Yu., Filinova A.S. Intrusion detection in computer networks (network anomalies). Textbook for universities. Moscow. Hotline - Telecom 2018.
[2] Yarochkin V.I. Information Security. Textbook for university students. - M.: Academic Project; Gaudeamus, 2nd ed. 2004. –544 s.
[3] Astrakhov A.V., Klimov S.M., Sychev M.P. "Countering computer attacks. Technological basis. " Electronic educational publication Moscow. 2013 MSTU named after N.E. Bauman
[4] Gulyaev VR, Computer viruses - a problem of the 21st century. Young scientist No. 1 (10) February 2017
[5] Kaspersky K. Notes of a computer virus researcher. - St. Petersburg: Peter, 2006.