**International Journal of Academic Engineering Research (IJAER)**
**ISSN: 2643-9085**
**Vol. 5 Issue 1, January - 2021, Pages: 24-28**

# Organizing Internet Protection

**Usmonov Makhsud**

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
***maqsudusmonov22@gmail.com***

***Abstract:*** *The advent of Internet technology has increased the ability to access information from a variety of sources quickly and easily to an unprecedented extent for everyone - from the average citizen to large organizations. Government agencies, science and education institutions, commercial enterprises and individuals began to create and store information in electronic form. This environment offers great convenience compared to previous physical storage: storage is very compact, transmission takes place instantly, and the possibilities of accessing rich databases over the network are very wide. The ability to use information effectively has led to a rapid increase in the amount of information.*

**Keywords:** FedCIRC, NIST, Information theft, key management, security, network management.

## INTRODUCTION

1. The problem of information security

2. Facts and figures

3. Areas of information security

4. Practical recommendations

The problem of information security The creation of Internet technologies has increased the opportunities for quick and easy access to information from a variety of sources for everyone - from ordinary citizens to large organizations. Government agencies, science and education institutions, commercial enterprises and individuals began to create and store information in electronic form. This environment offers great convenience compared to previous physical storage: storage is very compact, transmission takes place instantly, and the possibilities of accessing rich databases over the network are very wide. The ability to use information effectively has led to a rapid increase in the amount of information. Business in a number of commercial areas today considers information to be its most valuable asset. This is definitely a very positive development when it comes to the media and information that everyone can know. But Internet technologies for covert and confidential information flows have created new challenges as well as conveniences. The threat to information security in the Internet environment has increased dramatically: • Information theft • Violation of information content, unauthorized alteration of the owner • Pricketing into the network and servers Network hacking: first forwarding of received transactions (integrated sequence of actions), "refusal of service or interference with information", redirection of shipments in an unauthorized way. Ensuring information security involves addressing the following three key issues. These are: • Confidentiality • Integrity • Availability 2. Facts and Figures. According to a 1999 computer crime survey conducted by the U.S. Institute of Computer Security and the FBI, 57 percent of organizations surveyed said their Internet connection was "a place where most attacks occur," and 30 percent said it was. and 26 percent reported that secret information was stolen during the attack. According to the U.S. Federal Center for Computer Crime - FedCIRC, in 1998, about 130,000 government networks with 1,100,000 computers were compromised. "Computer hacking" refers to the launch of a special program by people to gain unauthorized access to a computer. Forms of organizing such aggression are different. They are divided into the following types

## METHODS

• Remote access to the computer: Software that allows you to access the Internet or the Internet anonymously • Access to the computer you are working on: based on anonymous access to the computer. • Do not use the computer remotely: on the basis of programs that connect to the computer remotely via the Internet (or network) and stop it or some of its programs (it is enough to restart the computer to start). • Do not use the computer you are working on: with disable software. • armoqNetwork Scanners: The network is actually a network of data-gathering software to determine which of the computers and programs running on the

network are vulnerable to intrusion. • topishFind software vulnerabilities: Through programs that search for vulnerabilities among large groups of computers on the Internet. • Decrypt: by means of programs that search for passwords that can be easily found in password files. • Net Analyzers (snifferers): through software that listens to network traffic. They have the ability to automatically separate user names, passwords, credit card numbers from traffic. The most common attacks have the following statistics: An analysis of 237 computer attacks conducted by NIST in 1998 was published on the Internet: • 29% of attacks occurred in the Windows environment. Lesson: Unix alone is not dangerous. • 20% of aggressors are remote networkers q elements (routers, switches, hosts, printers, firewalls). Lesson: Hosts can be accessed remotely without notice. • 5% of attacks were successful against routers and firewalls. Lesson: Internet network infrastructure developers do not have enough resistance to computer attacks. • 4% of attacks are organized to find free hosts that can withstand Internet aggression. Lesson: It is good that system administrators themselves regularly scan their hosts. • 3% of attacks are organized by websites against their users. Lesson It is not safe to search for information on the WWW. 1999 on the Internet. the most common computer attacks in March. Sendmail (oldest program), ICQ (complex "I'm looking for you" program, used by about 26 million people), Smurf (program that works with ping-packages), Teardrop (error-sensitive program), IMAP (mail program), Back Orifice ( the Trojan horse, for remote control of Windows 95/98), Netbus (similar to Back Orifice), WinNuke (can completely shut down Windows 95) and Nmap (scanning software). With the help of WinNuke, Papa Smurf and Teardrop programs, malicious people can attack and damage your computer. 3. Directions of information security The international standard NIST 7498-2 defines the basic security services. Its task is to determine the security direction of the open system communication model. These are: • Authentication. Identify a computer or network user;

• Access Access control. Verify and ensure user access to the computer network; • Data integrity. Checking the contents of the database for accidental or intentional unauthorized alterations; • Information confidentiality. Protecting Content from Unauthorized Disclosure • Neoproverjimost. Prevent the sender from refusing to acknowledge that the array was sent or received by the recipient. Many additional services (audit, access) and support services (key management, security, network management) serve to complement this basic security system. The complete security system of the Web site must cover all of the above security areas. Appropriate security tools (mechanisms) should be included in the software product. Improving authentication involves addressing the shortcomings of reusable passwords, ranging from single-use passwords to high-tech biometric authentication systems. Items that users carry with them, such as special cards, special tokens or floppy disks, are much cheaper and safer. The unique, module code protected application module is also handy for this purpose. The public key infrastructure is also an integral part of Web node security. The distribution system (people, computers), which is used to ensure authentication, data integrity and confidentiality of information, publishes an electronic certificate with public key infrastructure (certificate publisher). It contains the user ID, its public key, any additional information for the security system, and the digital signature of the certificate publisher. Ideally, this system would create a chain of certificates for the user at any two points on Earth. This chain allows someone to sign a secret letter, transfer money to an account or enter into an electronic contract, and for someone else - to check the source of the document and the identity of the signatory. NIST is working with several other organizations in this direction. Networks have set up firewalls, even though Internet networks have blocked open communication due to hacker attacks. There would be no open network without perfect software like PGP. 4. Practical recommendations Protecting the network from computer intrusions is a constant and intractable problem. But with a number of simple protections, most intrusions into the network can be prevented. For example, a well-configured firewall and antivirus software installed on each workstation (computer) will prevent most computer attacks. The following are 14 practical tips for protecting the Internet. 1. The security policy should be clear and concise. There should be rules and procedures in place to ensure that Internet security is set in a clear and consistent manner. The more secure a network security system is, the more secure its most vulnerable space is. An organization doi If there are several networks with different security policies, one network may lose its reputation due to the poor security of the other network.

Organizations should adopt a security policy so that the expected level of protection is the same everywhere. The most important aspect of the policy is the development of a single requirement for traffic through firewalls. The policy should also specify which security tools (e.g., intrusion detection tools or vulnerability scanners) in the network and how they should be used, and define standard secure configurations for different types of computers to achieve a single level of security. 2. Use a firewall (firewalls, English screen). This is the organization's most basic means of protection. Controls incoming and outgoing traffic (information flow) to the network. It can block or control any type of traffic. A well-configured brawmauer can repel most computer attacks. firewalls, smart cards and other hardware and software protection tools should be used wisely. 3. Brandmauer and WWW-servers should be tested for their resistance to threats of downtime. Attacks aimed at shutting down a computer are common on the Internet. Attackers are constantly shutting down WWW sites, overloading computers with redundant tasks, or filling networks with meaningless packages. This type of aggression can be very serious, especially if the attacker is smart at the level of organizing ongoing aggression. Because the source of this cannot be found. Networks concerned about their safety may organize attacks on themselves to estimate the damage that would result from such attacks. It is advisable to conduct such analyzes only by experienced system administrators or specialized consultants. 4. Cryptosystems should be widely used. Attackers often infiltrate the network by listening to traffic passing through its important locations by separating users from the traffic and their passwords.

Therefore, connections to remote machines must be encrypted when they are password protected. This is especially necessary when the connection is made through Internet channels or when connected to an important server. There are commercial and free programs for encrypting TCP / IP (the most popular SSH) traffic. Their use prevents aggression. The most reliable means of protecting the flow of information and resources on the Internet, combined with the Internet environment, is the joint use of symmetric and symmetric cryptosystems. 5. Computers should be configured competently from a security standpoint. When operating systems are reinstalled on a computer, they are often vulnerable to intrusion. This is because when the operating system is initially installed, all network tools are allowed to be used and cannot be used properly. This allows the attacker to use many methods to attack the car. Therefore, all unnecessary network tools should be disconnected from the computer. 6. Patching. Companies make corrections to fix bugs found in their bots. If these errors are not corrected, the attacker can use it to attack your program and through it your computer. System administrators must first protect the necessary hosts by installing fixes to programs on their most essential systems. This is because fixes occur frequently and you may not have time to install them on all computers. Generally, adjustments should only be made by the company that developed the software. Definitely fix the defects encountered in Internet network security. They should also use the other protective equipment listed below.

7. Intrusion Detection should be used. Aggression detection systems detect aggression by operational detection. They are placed behind the firewall to detect intrusions from within the network, and to detect intrusions to the firewall. Such tools have different capabilities. More information can be found on the following site.

http://www.icsa.net/services/consortia/intrusion/educational_material.shtml 8. It is important to try to detect viruses and "Trojan horse" programs in a timely manner. Antivirus software is an integral part of protection for the security of any network. They monitor computer operation and find malicious programs. The only problem they cause is that they must be installed on all computers on the network and regularly updated to ensure maximum protection. It takes a long time to do this, but otherwise the engine will not give the expected effect. Computer users need to be taught how to do this, but they just need to not be left with the task completely. In addition to anti-virus software, you should also scan applications for emails on the mail server. In this way, the path of viruses that can reach users' computers is blocked. 9. The tolerant spaces should be scanned. Such scanning software scans the network to find computers that are vulnerable to certain types of intrusions. They have a large database of vulnerabilities, which can be used to find out if there is a vulnerability on one computer or another. Commercial and free scanners are available. System administrators should periodically find such computers on their own networks in a timely manner and take appropriate action against such networks. The risk level should be assessed to identify vulnerabilities in the protection of individual devices. 10. It is necessary to determine the network topology and run port scanners. Such programs provide a complete picture of how the network is structured, what computers work on it, what services are performed on each machine. Attackers use these programs to detect vulnerable computers and programs. Network administrators also use such software to determine which programs are running on which computers on their networks. This is a good tool for finding misconfigured computers and fixing them. 11. Use Password Crackers. Hackers often try to use computers to steal encrypted files with passwords. They then run special programs that decrypt them and use them to find the empty passwords in these encrypted files. Once such a password is obtained, they use different methods of accessing the computer without notifying the computer and the network like a normal user. Although this tool is used by malicious people, it is also useful for the system administrator. System administrators should periodically find such passwords to their encrypted files in a timely manner and find appropriate passwords to take appropriate action. 12. Be wary of war dialers. Users are often allowed to receive incoming phone calls to their computers by bypassing the organization's network protection tools. They sometimes set up their own programs to connect the modem to the computer from home by connecting it to the modem before returning from work. Attackers combat communication

they try to call many phone numbers using installation software and thus infiltrate such networks, allowing access from the outside via a modem. Because users often configure their computers themselves, such computers are poorly protected from intrusions, creating another opportunity for network intrusion. System administrators should regularly use combat communication installers to check the phone numbers of their users and take timely action to find computers configured accordingly. There are commercial and free distributed combat communication software. 13. It is important to be aware of and follow security advisories in a timely manner. Security Recommendations are warnings that computer crime teams and software developers will issue warnings about dangerous areas of the program that will soon be discovered. The recommendations are very helpful, take very little time to read, and warn of the most serious dangers that can occur due to overlooked hazardous areas. They express the risk and give tips to prevent it. They can be obtained from a number of places. The two most useful recommendations are the ones published by the Computer Crime Group and can be found on the CIAC and CERT sites. 14. The security incident investigation team should operate on a regular basis. Security-related incidents can occur in any network (even if there is a false alarm). Employees of the organization must know in advance what to do in this or that case. In what cases to apply to law enforcement agencies you need to call a computer crime team and in which cases you need to disconnect the network from the Internet and what to do when the lock of an important server is broken. CERT provides advice in this regard within the United States. FedCIRC is responsible for providing advice to U.S. public and government organizations. It is advisable to have such counseling centers in every state.

Additional information about computer attacks can be found in the following article on some of the programs designed to attack. General computer security information can be obtained from: • manNIST Computer Security Resource Clearinghouse • Federal Computer Incident Response Capability • Center for Education and Research in Information Assurance and Security • Carnegie Mellon Emergency Response Team The traditional approaches and tools used in mining are no longer sufficient. In this context, the importance of cryptography, the most reliable and tested method of information protection, has increased. Below we will discuss in detail the cryptological direction of information protection on the Internet and the Internet.

## RESULTS

• Remote access to the computer: Software that allows you to access the Internet or the Internet anonymously • Access to the computer you are working on: based on anonymous access to the computer. • Do not use the computer remotely: on the basis of programs that connect to the computer remotely via the Internet (or network) and stop it or some of its programs (it is enough to restart the computer to start). • Do not use the computer you are working on: with disable software. • armoqNetwork Scanners: The network is actually a network of data-gathering software to determine which of the computers and programs running on the network are vulnerable to intrusion. • topishFind software vulnerabilities: Through programs that search for vulnerabilities among large groups of computers on the Internet. • Decrypt: by means of programs that search for passwords that can be easily found in password files. • Net Analyzers (snifferers): through software that listens to network traffic. They have the ability to automatically separate user names, passwords, credit card numbers from traffic. The most common attacks have the following statistics: An analysis of 237 computer attacks conducted by NIST in 1998 was published on the Internet: • 29% of attacks occurred in the Windows environment. Lesson: Unix alone is not dangerous. • 20% of aggressors are remote networkers q elements (routers, switches, hosts, printers, firewalls). Lesson: Hosts can be accessed remotely without notice. • 5% of attacks were successful against routers and firewalls. Lesson: Internet network infrastructure developers do not have enough resistance to computer attacks. • 4% of attacks are organized to find free hosts that can withstand Internet aggression. Lesson: It is good that system administrators themselves regularly scan their hosts. • 3% of attacks are organized by websites against their users. Lesson It is not safe to search for information on the WWW. 1999 on the Internet. the most common computer attacks in March. Sendmail (oldest program), ICQ (complex "I'm looking for you" program, used by about 26 million people), Smurf (program that works with ping-packages), Teardrop (error-sensitive program), IMAP (mail program), Back Orifice ( the Trojan horse, for remote control of Windows 95/98), Netbus (similar to Back Orifice), WinNuke (can completely shut down Windows 95) and Nmap (scanning software). With the help of WinNuke, Papa Smurf and Teardrop programs, malicious people can attack and damage your computer. 3. Directions of information security The international standard NIST 7498-2 defines the basic security services. Its task is to determine the security direction of the open system communication model. These are: • Authentication. Identify a computer or network user;

## DISCUSSION

7. Intrusion Detection should be used. Aggression detection systems detect aggression by operational detection. They are placed behind the firewall to detect intrusions from within the network, and to detect intrusions to the firewall. Such tools have different capabilities. More information can be found on the following site.

http://www.icsa.net/services/consortia/intrusion/educational_material.shtml 8. It is important to try to detect viruses and "Trojan horse" programs in a timely manner. Antivirus software is an integral part of protection for the security of any network. They monitor computer operation and find malicious programs. The only problem they cause is that they must be installed on all computers on the network and regularly updated to ensure maximum protection. It takes a long time to do this, but otherwise the engine will not give the expected effect. Computer users need to be taught how to do this, but they just need to not be left with the task completely. In addition to anti-virus software, you should also scan applications for emails on the mail server. In this way, the path of viruses that can reach users' computers is blocked. 9. The tolerant spaces should be scanned. Such scanning software scans the network to find computers that are vulnerable to certain types of intrusions. They have a large database of vulnerabilities, which can be used to find out if there is a vulnerability on one computer or another. Commercial and free scanners are available. System administrators should periodically find such computers on their own networks in a timely manner and take appropriate action against such networks. The risk level should be assessed to identify vulnerabilities in the protection of individual devices. 10. It is necessary to determine the network topology and run port scanners. Such programs provide a complete picture of how the network is structured, what computers work on it, what services are performed on each machine. Attackers use these programs to detect vulnerable computers and programs. Network administrators also use such software to determine which programs are running on which computers on their networks. This is a good tool for finding misconfigured computers and fixing them. 11. Use

Password Crackers. Hackers often try to use computers to steal encrypted files with passwords. They then run special programs that decrypt them and use them to find the empty passwords in these encrypted files. Once such a password is obtained, they use different methods of accessing the computer without notifying the computer and the network like a normal user. Although this tool is used by malicious people, it is also useful for the system administrator. System administrators should periodically find such passwords to their encrypted files in a timely manner and find appropriate passwords to take appropriate action.

## CONCLUSION

The problem of information security The creation of Internet technologies has increased the opportunities for quick and easy access to information from a variety of sources for everyone - from ordinary citizens to large organizations. Government agencies, science and education institutions, commercial enterprises and individuals began to create and store information in electronic form. This environment offers great convenience compared to previous physical storage: storage is very compact, transmission takes place instantly, and the possibilities of accessing rich databases over the network are very wide. The ability to use information effectively has led to a rapid increase in the amount of information. Business in a number of commercial areas today considers information to be its most valuable asset. This is definitely a very positive development when it comes to the media and information that everyone can know. But Internet technologies for covert and confidential information flows have created new challenges as well as conveniences.

## REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

3Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

4 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.

5 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

6 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.