Remote Computer Management System

Kutay Koray 1,\* , Yakup Kaan Ekşi 2 ve Emre Olca 3

1 Maltepe Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği, İstanbul

2 Maltepe Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği, İstanbul

3 Maltepe Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği, İstanbul

\* Sorumlu yazar: kutaykoray58@gmail.com

Özet

Bu çalışma, bilgisayar ağları içinde yönetim amaçlarıyla hedef bilgisayarlara uzaktan erişimi sağlamayı amaçlayan Uzaktan Bilgisayar Yönetim Sistemi'nin tasarımı ve geliştirilmesine odaklanmaktadır. Projenin birincil amacı, kullanıcıların hedef bilgisayarlarda çeşitli işlemler yapabilmesini sağlayarak bilgisayar ağları içinde uzaktan erişimi kolaylaştırmaktır. Bu hedefe ulaşmak için, proje belirli bir port üzerinde dinleme yapacak ve gelen bağlantıları kabul edecek bir soket dinleyici oluşturulmasını içerecektir. Ardından, hedef bilgisayara bir arka kapı açabilen gizli bir ajan yazılımı yerleştirilecektir. Bu yazılım aracılığıyla, hedef bilgisayarda bir kabuk (Shell) kurulacak ve kullanıcılara komutları yürütme yetkisi verilecektir. Sonuç olarak, kullanıcılar hedef bilgisayarda komutları yürütebilecek, çeşitli bilgileri toplayabilecek ve bunları belirlenen bir veri tabanına iletebilecektir. Proje boyunca, kullanıcıların beklentilerini karşılamak amacıyla fonksiyonel, performans ve güvenlik gereksinimlerine titizlikle dikkat edilecektir.

**Anahtar kelimeler:** Uzaktan Bilgisayar Yönetimi, Siber Güvenlik, Bilgisayar Kriminalistiği, Ağ Güvenliği, Veri Koruma.

Remote Computer Management System

Abstract

This study focuses on designing and developing a Remote Computer Management System to enable remote access to target computers for administrative purposes within computer networks. The primary goal of the project is to simplify remote access within computer networks, allowing users to perform various operations on target computers. To achieve this, the project will involve creating a socket listener that will listen on a specified port and accept incoming connections. Then, a covert agent software capable of opening a backdoor will be deployed onto the target computer. This software will establish a shell on the target computer, granting users the authority to execute commands. As a result, users will be able to run commands on the target computer, gather various pieces of information, and transmit them to a designated database. Throughout the project, careful attention will be given to addressing the functional, performance, and security requirements to meet the users' expectations.

**Key words:** Remote Computer Management, Cybersecurity, Computer Forensics, Network Security, Data Protection.

1. Giriş

Today, cybersecurity and digital forensics have become very important due to increasingly complex threats and rising data breaches. Attacks on computer networks endanger both personal and corporate data, which requires continuous improvement of security measures. In this context, remote computer management systems have become crucial tools for network administrators and security experts, providing direct access and control over target computers.

This study focuses on the design and development of a Remote Computer Management System that aims to enhance cybersecurity and digital forensics capabilities by facilitating remote access and management of target computers. The system includes creating a socket listener that accepts connections on a specified port and deploying a covert agent software that can open a backdoor on the target computer. This allows users to execute commands, gather information, and transmit this data to a centralized database. Our project offers higher security and performance compared to existing remote access systems, bringing a significant innovation to this field.

According to the data, [1] working remotely helps people understand more about cybersecurity and encourages them to take safety measures. When people follow information security policies, it helps control this effect. Also, as people become more aware of cybersecurity, they tend to take more safety measures. This study adds to what we know about how people act to protect themselves online and gives managers tips on dealing with the increasing cybersecurity threats when people work remotely.

This study [2] explores remote computer forensics, while our project focuses on remote computer management systems. Both enable access and management without physical presence, addressing the efficient delivery of digital forensic capabilities to remote locations. They share a common goal of achieving effective results through technological tools and methods.

In this paper, we will first provide detailed information about the system's overall architecture and the technologies used. Then, we will discuss the system's functionality, performance, and security measures. Finally, the conclusion will offer an overall assessment of the project and suggest directions for future work.

2. Materyal ve Metot

2.1. Command and Scripting Interpreter ( T1059)

Purpose = Selected MITRE ATT&CK techniques enable unauthorized access and control of computer systems. Attackers utilize command and scripting interpreters like Windows Command Shell, Unix Shell, and Python to execute malicious commands and scripts. This poses serious security threats, including data theft, privilege escalation, and system manipulation..

2.2. File and Directory Discovery (T1083)

Purpose = The purpose of employing the MITRE ATT&CK technique "File and Directory Discovery (T1083)" is to gather information about the file system structure and contents on a compromised system. Attackers use this technique to identify valuable files and sensitive data for further exploitation, aiding in data exfiltration or lateral movement within the organization's network.

2.3. File and Directory Discovery (T1083)

Purpose = The goal of utilizing the MITRE ATT&CK technique "Data from Local System (T1005)" is to acquire information stored locally on the compromised system. Attackers employ this technique to gather sensitive data, including credentials, configuration details, or proprietary information, for subsequent use in their malicious activities. By accessing data from the local system, adversaries can escalate privileges, perform reconnaissance, or exfiltrate valuable information, posing significant security risks to the targeted organization.

2.4. Exfiltration Over Alternative Protocol (T1048)

Purpose = The purpose of the MITRE ATT&CK technique "Exfiltration Over Alternative Protocol (T1048)" is to secretly transfer data from compromised systems using non-standard communication channels. Attackers employ this method to avoid detection by conventional security measures, facilitating the unauthorized extraction of sensitive information.

2.5. Metot

In this project, we followed these steps to develop a remote computer management system: identifying requirements, designing, developing, testing, and deploying. We used Python programming language for design and development, tested it in a local network, and improved the system based on feedback before successful deployment [4].

ekran görüntüsü, diyagram, metin, plan içeren bir resim

Açıklama otomatik olarak oluşturuldu2.6. Sequence Diagram

ekran görüntüsü, diyagram, metin, plan içeren bir resim

Açıklama otomatik olarak oluşturuldu2.7. High-Level Diagram

2.8. Web Interface

ekran görüntüsü, tasarım içeren bir resim

Açıklama otomatik olarak oluşturuldu

2.9. Technological Level

The project leverages a selection of libraries and frameworks within the Python programming ecosystem, reflecting a moderate level of technological sophistication. Here is an overview of the utilized libraries and technologies:

* Python: The primary programming language chosen for project development.
* Socket: Employed for facilitating network communication, enabling the establishment and management of network connections.
* JSON: Integrated for its capabilities in serializing and deserializing data structures, providing a means to represent complex data in a human-readable format.
* Base64: Implemented for encoding binary data into ASCII characters and vice versa, serving purposes such as secure transmission and storage of binary information.
* SQLite3: Adopted as the relational database management system, offering lightweight, local storage for the project's data needs.
* Flask: Chosen as the web framework for developing web applications in Python, enabling the creation of server-side logic and dynamic web pages.

2.10. Functional Requariments

* The user should be able to create a socket listener listening on a specific port.
* The user should be able to install an agent software on the target computer capable of opening a backdoor.
* The user should be able to run the agent software on the target computer. The user should be able to create a shell on the target computer. The user should be able to send and receive commands through the shell on the target computer.
* The user should be able to transfer collected information about the target computer to a database.

2.11. Performance Requariments

* The socket listener should respond quickly to clients.
* The agent software should operate with low system resources on the target computer and remain undetected.
* Command execution and result retrieval through the shell should be fast and reliable.
* Information transfer to the database should be fast and reliable.

3. Bulgular

The developed remote computer management system has been successfully tested and utilized. Test results indicate that the system meets performance expectations and features a user-friendly interface. Furthermore, it has been observed that the system operates reliably and swiftly in a local network environment. User feedback confirms that the system is easily understandable and usable by users. In conclusion, the developed system has demonstrated its effectiveness as a valuable tool in remote computer management [6].

3.1. Extracted Data

metin, ekran görüntüsü, sayı, numara, yazılım içeren bir resim

Açıklama otomatik olarak oluşturuldu

4. Sonuçlar

In summary, the project represents a significant endeavor in cybersecurity, utilizing the MITRE ATT&CK framework and advanced techniques to assess vulnerabilities in computer systems. By implementing listener and backdoor mechanisms, it effectively simulates realistic attack scenarios, highlighting the critical importance of robust defensive measures [3]. The project's technical proficiency, modular design, and adherence to Agile methodologies underscore its contribution to proactive cybersecurity efforts [5], emphasizing the need for continual vigilance and adaptation in safeguarding digital assets against evolving threats.

Kaynaklar

[1]. Joseph K. Nwankpa , Pratim Milton Datta (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. Computers & Security Volume 130, July 2023, 103266.

[2]. K. U. maheswari and G. Shobana, "The State of the art tools and techniques for remote digital forensic investigations," 2021 3rd International Conference on Signal Processing and Communication (ICPSC), Coimbatore, India, 2021, pp. 464-468, doi: 10.1109/ICSPC51351.2021.9451718.

[3]. H. Huang and J. Li, "Research on Network Communication Model and Network Security Technology through Big Data," 2021 IEEE International Conference on Data Science and Computer Application (ICDSCA), Dalian, China, 2021, pp. 138-141, doi: 10.1109/ICDSCA53499.2021.9650308.

[4]. J. Wijekoon, M. Wijesundara, T. Dassanayaka, D. Samarathunga, R. Dissanayaka and D. Perera, "The Advanced Remote PC Management Suite," 2011 6th International Conference on Industrial and Information Systems, Kandy, Sri Lanka, 2011, pp. 410-413, doi: 10.1109/ICIINFS.2011.6038103.

[5]. M. M. Losavio and D. W. Keeling, "Computer Forensics And Electronic Evidence - Failure of Competent Computer Forensic Analysis And Other Computer-Related Acts As Ineffective Assistance Of Counsel," 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA, 2011, pp. 1-6, doi: 10.1109/SADFE.2011.6.

[6]. B. K. Sharma, M. A. Joseph, B. Jacob and B. Miranda, "Emerging trends in Digital Forensic and Cyber security- An Overview," 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, 2019, pp. 309-313, doi: 10.1109/ITT48889.2019.9075101.