

SeroXen Documentation

Written By C5





SeroXen TOS | Part 1

- Terms of Service for SeroXen:
- Introduction: Welcome to SeroXen. By using our remote administration tool, you agree to comply with the terms and conditions set forth in this document. Failure to comply with these terms and conditions may result in the permanent suspension of your account.
- Legal and Ethical Use: SeroXen is designed for legal and ethical use only. The use of SeroXen for illegal or unethical purposes is strictly prohibited. The owner of SeroXen cannot be held responsible for any illegal or unethical activities that you may engage in while using SeroXen. It is your responsibility to use SeroXen in a legal and ethical manner.

SeroXen TOS | Part 2

- Prohibited Activities: The following activities are strictly prohibited while using SeroXen:
 - Hacking into systems without the owner's consent
 - Distributing malware, viruses, or other harmful software
 - Stealing personal information
 - Using SeroXen for espionage or surveillance purposes
 - Using SeroXen to harass or intimidate others
 - Engaging in any illegal or unethical activities

SeroXen TOS | Part 3

- Consequences of Prohibited Activities:
 - If you engage in any prohibited activities while using SeroXen, your account will be permanently suspended, and you will be banned from purchasing a SeroXen license again. We reserve the right to report illegal activities to the appropriate authorities.
- Cracking and Promotion of Cracked Software: Attempting to crack or modify SeroXen is strictly prohibited. We take the protection of our software very seriously, and any attempts to modify, reverse engineer, or crack SeroXen will result in the permanent suspension of your account. Additionally, promoting or distributing cracked versions of SeroXen is also strictly prohibited and will result in the same consequences.
- Account Security: It is your responsibility to keep your SeroXen account secure. You are responsible for maintaining the confidentiality of your login credentials, and you should not share your account information with anyone. You are responsible for all activities that occur under your account, and you agree to notify us immediately if you suspect any unauthorized access to your account.

SeroXen TOS | Part 4

- Termination of Service: We reserve the right to terminate your access to SeroXen at any time, without notice, if we suspect that you are engaging in illegal or unethical activities, or if you violate any of the terms and conditions set forth in this document.
- Disclaimer: The owner of SeroXen cannot be held responsible for any damages or losses that you may incur while using SeroXen. By using SeroXen, you acknowledge that you are using the software at your own risk, and that you are responsible for any consequences that may arise from your use of the software.
- SeroXen is intended for legal and ethical use only. Any illegal or unethical use of the software is strictly prohibited. Examples of prohibited activities include but are not limited to: hacking into systems without proper authorization, accessing or tampering with confidential data, using the software for phishing attacks, or engaging in any activity that violates local, state, or federal laws.

SeroXen TOS | Part 5

- The use of SeroXen to target individuals or entities without their explicit consent is strictly prohibited. The user is solely responsible for obtaining any necessary consent before using the software on any system or network.
- SeroXen should not be used to engage in any form of cyberbullying or harassment. Any activity that is intended to harass, defame, or harm another individual or entity is strictly prohibited.
- The user is solely responsible for their actions while using SeroXen. The owner and developers of the software shall not be held responsible for any damages, legal or otherwise, that may result from the user's use of the software.

SeroXen TOS | Part 6

- The owner reserves the right to terminate a user's license and ban them from using the software in the event of a violation of the terms of service. The user will not be entitled to a refund in the event of a license termination due to a violation of the terms of service.
- Any attempt to modify, reverse engineer, or crack the software is strictly prohibited. The user shall not attempt to modify or create any derivative works of the software, nor shall they attempt to distribute or promote any modified or cracked versions of the software.
- The user shall not use SeroXen to gain unauthorized access to any system or network, nor shall they attempt to use the software in any manner that could result in damage to any system or network.

SeroXen TOS | Part 7

- The owner and developers of SeroXen reserve the right to modify or update the terms of service at any time. The user is responsible for regularly reviewing the terms of service and abiding by any changes or updates.
- The owner and developers of SeroXen shall not be held liable for any damages, direct or indirect, that may result from the use of the software.
- By purchasing and using SeroXen, the user agrees to be bound by the terms of service outlined in this document. The user is responsible for understanding and abiding by the terms of service at all times while using the software.
- These terms and conditions are intended to promote the legal and ethical use of SeroXen as a remote administration tool. Any violation of these terms and conditions may result in the termination of the user's license and/or legal action.

SeroXen TOS | Part 8

- Sharing the download link or any of the SeroXen files is strictly prohibited. Users are prohibited from distributing, publishing, or sharing any part of the software. Any user found to be sharing the download link or any of the SeroXen files will have their account permanently banned and will not be able to purchase a license again.
- Users are prohibited from attempting to infect other SeroXen users with SeroXen or any other type of malicious software. Any user found to be attempting to infect other SeroXen users will have their account permanently banned and will not be able to purchase a license again.
- Users are prohibited from uploading the SeroXen Client File or any of the SeroXen files to manual submission of antivirus companies. Any user found to be uploading the SeroXen Client File or any of the SeroXen files to manual submission of antivirus companies will have their account permanently banned and will not be able to purchase a license again.

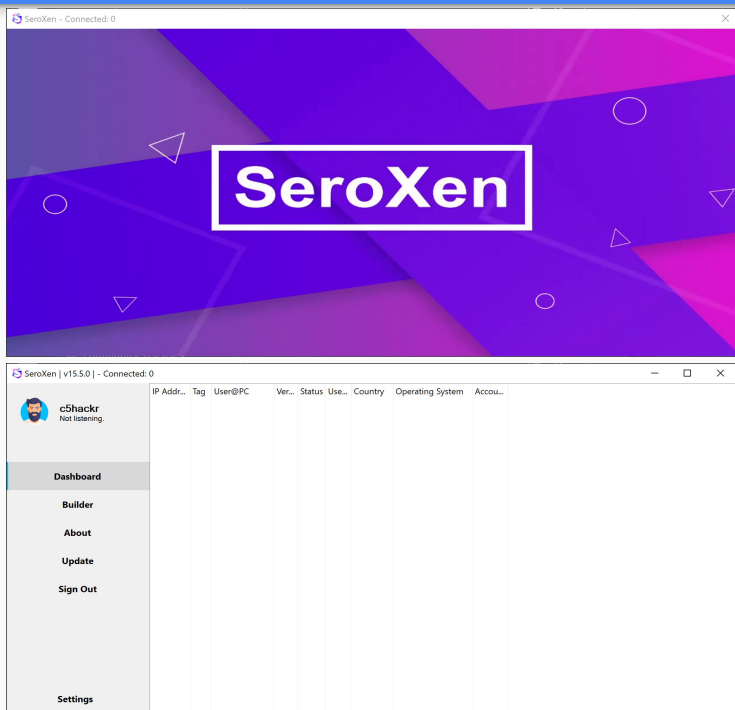
SeroXen TOS | Part 9

- Users are prohibited from making malicious plugins for use with SeroXen. Any user found to be creating malicious plugins will have their account permanently banned and will not be able to purchase a license again.
- Users are prohibited from sharing their SeroXen account login information, account details, or license with anyone else. Any user found to be sharing their SeroXen login information, account details, or license will have their account permanently banned and will not be able to purchase a license again.
- SeroXen reserves the right to permanently shutdown the service at any time, without notice or refunds. Users acknowledge that SeroXen is not responsible for any losses or damages that may result from the shutdown of the service.

SeroXen TOS | Conclusion

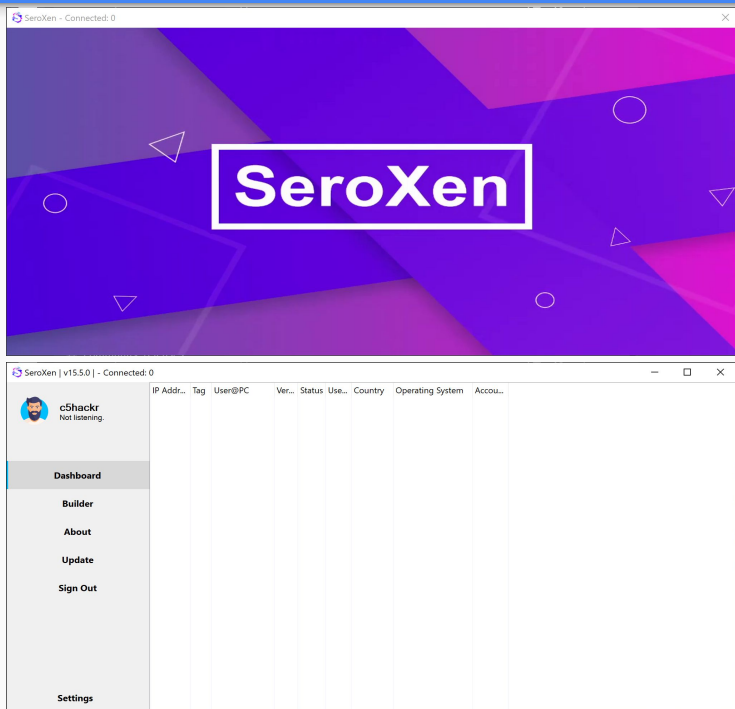
- Conclusion: By using SeroXen, you agree to comply with the terms and conditions set forth in this document. Failure to comply with these terms and conditions may result in the permanent suspension of your account. If you have any questions or concerns regarding the terms and conditions, please contact us on the website live support chat or the SeroXen discord.

What is SeroXen? | Part 1



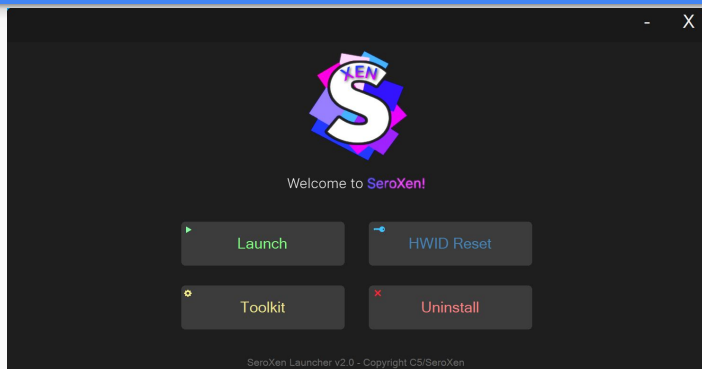
- SeroXen is a remote administration tool that is designed to allow remote access and control of a target system. It is a heavily modified version of the Quasar remote administration tool, which is an open-source, multi-platform remote administration tool that allows remote access and control of a Windows system.
- The modifications made to Quasar to create SeroXen are extensive and include the addition of several new features, as well as modifications to existing features to enhance their functionality and improve their performance. For example, SeroXen includes a C# unrestricted execution based plugin system, which allows users to execute any C# code on the server and the client. This is a powerful feature that allows users to extend the functionality of SeroXen beyond what is included in the core software.
- SeroXen also includes a rootkit feature, which is designed to make it difficult for the software to be detected and removed from a target system, enhancing its stealth capabilities and making it more difficult for attackers to maintain persistent access.

What is SeroXen? | Conclusion



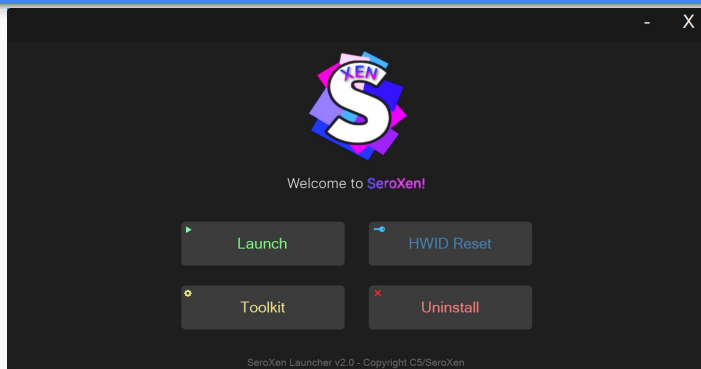
- Other features of SeroXen include remote desktop control, HVNC (Strictly For Pentesting ONLY), file management, startup management, TCP connections, registry editing, password recovery, keylogging, and more. These features allow users to remotely manage and control a target system, making it a powerful tool for system administrators and others who need to manage remote systems.
- Overall, SeroXen is a highly capable and powerful remote administration tool that is designed to provide users with extensive remote access and control capabilities. Its heavily modified Quasar codebase and extensive feature set make it a popular choice among system administrators and others who need to manage remote systems.

SeroXen Launcher | Part 1



- **Launch SeroXen:** The primary feature of the SeroXen launcher is its ability to launch SeroXen itself. SeroXen is an application designed to help users manage and optimize their computer systems. It provides a range of tools and utilities, Remote Desktop, Registry Editor, and more. By launching SeroXen using the launcher, users can easily access these features.
- **HWID Account Lock Reset:** Another important feature of the SeroXen launcher is its ability to reset HWID account locks. HWID (Hardware Identification) is a unique identifier associated with a user's computer hardware. Some software applications use HWID to restrict access and prevent unauthorized use. However, if a user's HWID is locked, they may be unable to access the software even if they have a valid license. The SeroXen launcher can reset HWID account locks, allowing users to access the software they have licensed.

SeroXen Launcher | Conclusion



- **SeroXen Toolkit:** The SeroXen launcher also provides access to the SeroXen toolkit. The toolkit is a collection of tools and utilities that can help users manage and optimize their usage with SeroXen. Some of the tools available in the SeroXen toolkit include Build2Exe (Free), Build2Lnk (3 Credits), Build2Exe [Binder] (1 Credit). By accessing the toolkit through the launcher, users can easily access these tools.
- **SeroXen Uninstall Feature:** Finally, the SeroXen launcher also provides a feature for uninstalling SeroXen. While SeroXen is a useful tool, some users may wish to uninstall it for various reasons. The SeroXen uninstall feature ensures that the software is removed from the user's system completely and without any leftover files or settings. This feature can be accessed easily through the SeroXen launcher.
- **Conclusion:** In summary, the SeroXen launcher offers several key features that can help users manage and optimize their computer systems. By providing access to the SeroXen toolkit, allowing users to launch SeroXen, resetting HWID account locks, and providing a simple uninstall feature, the launcher can help users make the most of their computing experience. Whether you're looking to optimize your system for better performance or simply need to reset an account lock, the SeroXen launcher is a valuable tool for any SeroXen user.

Core Features | Part 1

- SeroXen is a powerful remote access tool that offers a wide range of features to help users manage and control remote systems. The tool offers a variety of capabilities, including system information, file management, remote shell, password recovery, keylogging, remote desktop, and more. In this writeup, we will explore the features of SeroXen, discussing how they work and how they can be useful in managing remote systems.
- **System Information:** The system information feature of SeroXen allows users to view detailed information about the remote system they are accessing. This includes information about the operating system, hardware configuration, system processes, and more. This feature is useful for troubleshooting and diagnosing system issues remotely.
- **File Manager:** The file manager feature of SeroXen allows users to view and manage files on the remote system. This includes the ability to browse directories, upload and download files, delete files, and more. This feature is useful for transferring files between systems and managing remote files.

Core Features | Part 2

- **Startup Manager:** The startup manager feature of SeroXen allows users to view and manage startup programs on the remote system. This includes the ability to enable or disable startup programs and manage startup configurations. This feature is useful for optimizing system performance and ensuring that only necessary programs are running at startup.
- **Remote Shell:** The remote shell feature of SeroXen allows users to execute commands on the remote system using a command prompt interface. This feature is useful for performing system administration tasks remotely, such as running scripts and executing system commands.
- **TCP Connections:** The TCP connections feature of SeroXen allows users to view active network connections on the remote system. This includes information about the source and destination addresses, ports, and protocol used. This feature is useful for monitoring network activity and identifying potential security issues.

Core Features | Part 3

- **Reverse Proxy:** The reverse proxy feature of SeroXen allows users to set up a proxy server on the remote system. This can be used to redirect network traffic through the remote system, enabling users to bypass firewalls and access restricted resources. This feature is useful for testing network security and for accessing resources that are otherwise inaccessible.
- **Registry Editor:** The registry editor feature of SeroXen allows users to view and edit the Windows registry on the remote system. This includes the ability to add, delete, and modify registry keys and values. This feature is useful for configuring system settings remotely and troubleshooting registry-related issues.
- **Remote Execute:** The remote execute feature of SeroXen allows users to execute arbitrary code on the remote system. This feature is useful for performing complex system administration tasks remotely, such as installing and configuring software.

Core Features | Part 4

- Shutdown, Restart, Standby (Sleep Mode): The shutdown, restart, and standby features of SeroXen allow users to control the power state of the remote system. This feature is useful for managing system uptime and performing maintenance tasks remotely.
- Password Recovery: The password recovery feature of SeroXen allows users to recover passwords stored on the remote system. This includes passwords for web browsers, email clients, and other applications. This feature is useful for recovering lost passwords and for testing the security of password storage systems.
- Keylogger: The keylogger feature of SeroXen allows users to record keystrokes on the remote system. This includes information about the keys pressed, the application used, and the timestamp of the keystrokes. This feature is useful for monitoring user activity and for testing the security of password entry systems.

Core Features | Part 5

- Remote Desktop: The remote desktop feature of SeroXen allows users to view and control the remote desktop of the system. This includes the ability to view the screen, interact with applications, and control the mouse and keyboard. This feature is useful for performing remote support and for accessing systems that are not physically accessible. It can be used to troubleshoot issues and perform maintenance tasks on a remote system.
- HVNC: The HVNC feature of SeroXen allows users to view and control the remote desktop of the system without alerting the user that their screen is being viewed. This feature is strictly for pentesting only and should not be used for any illegal purposes. It can be used to test the security of a system by simulating a real-world attack, as of the time of this writeup SeroXen's HVNC currently supports the following browsers: Chrome, Edge, Brave, Firefox.
- Show MessageBox: The Show MessageBox feature of SeroXen allows users to display a message box on the remote system. This message can be customized and can be used to display important information or to notify users of upcoming system maintenance tasks.

Core Features | Part 6

- **Send to Website:** The Send to Website feature of SeroXen allows users to send information from the remote system to a specified website. This information can include system information, file information, and other data. This feature is useful for monitoring system activity and for gathering information for analysis.
- **Update SeroXen Client File:** The Update SeroXen client file feature of SeroXen allows users to update the client file of SeroXen on the remote system. This can be useful for updating the software to the latest version and for ensuring that the system is protected against known vulnerabilities.
- **Change Client Identification Tag:** The Change Client Identification Tag feature of SeroXen allows users to change the identification tag of the SeroXen client on the remote system. This can be useful for ensuring that the system is identified correctly.

Core Features | Part 7

- **Remove Offline Client:** The Remove Offline Client feature of SeroXen allows users to remove offline client logs from the remote system. This can be useful for maintaining system performance and for preventing the accumulation of unnecessary logs.
- **Reconnect:** The Reconnect feature of SeroXen allows users to reconnect to the remote system after a disconnection. This feature is useful for maintaining remote access to the system and for ensuring that system activity is not interrupted.
- **Uninstall SeroXen Client File:** The Uninstall SeroXen Client File feature of SeroXen allows users to remove the SeroXen client from the remote system. This can be useful for removing the tool from a system after its use has been completed.

Core Features | Part 8

- SeroXen is designed to be FUD (Fully Undetectable), meaning that it is not detected by antivirus software. This makes it easy to install and set up without having to disable or modify the system's antivirus settings.
- By being FUD, SeroXen ensures that the remote system remains safe and secure. Antivirus software is an essential tool for detecting and removing malicious software, but it can also interfere with legitimate software like SeroXen. By being FUD, SeroXen can also operate without triggering the antivirus software, avoiding false positives and ensuring that the remote system remains protected.

Core Features | Part 9

- Moreover, SeroXen's FUD feature also allows it to remain undetected by security software and firewalls, which makes it a useful tool for penetration testing and security analysis. It can help security professionals to identify and fix vulnerabilities in systems, networks, and applications, and thereby improve their security posture.
- In conclusion, SeroXen's FUD feature ensures easy installation and setup without having to mess around with the system antivirus settings, and also keeps the remote computer safe by avoiding detection by antivirus software.

Core Features | Part 10

- SeroXen has a feature that allows it to keep track of offline computers. This feature is useful in situations where the remote computer is not connected to the internet or is offline for an extended period of time.
- The offline client log feature in SeroXen allows it to store information about offline computers. When a remote computer goes offline, SeroXen will log relevant information about the system, such as the IP address and hostname.
- This feature is useful for system administrators who need to keep track of offline systems and ensure that they are up-to-date with the latest patches and updates. It allows them to identify systems that have not been online for an extended period and take appropriate action, such as performing maintenance tasks or scheduling a time to bring the system back online.

Core Features | Part 11

- In addition, the offline client log feature in SeroXen can be used to track the usage of remote systems over time. It allows administrators to monitor the frequency and duration of connections, which can be useful in identifying patterns and trends in system usage.
- In conclusion, the offline client log feature in SeroXen allows it to keep track of offline computers, which is useful for system administrators who need to monitor remote systems and ensure that they are up-to-date and secure. This feature enhances the overall functionality and usability of SeroXen, making it a valuable tool for managing and controlling remote systems.

Core Features | Part 12

- SeroXen has a rootkit that prevents it from being uninstalled by a normal user or a threat actor. A rootkit is a type of software that is designed to hide the existence of certain processes or programs from the operating system, and it is often used to maintain persistent access to a system.
- SeroXen's rootkit feature makes it difficult to detect and remove the software from a remote system. The rootkit is designed to be persistent, meaning that it will survive reboots and other system-level events.
- The rootkit also includes a self-defense mechanism that can detect and prevent attempts to remove the software. For example, if a user attempts to uninstall SeroXen using the normal Windows uninstaller, the rootkit will detect this and prevent the uninstallation process from completing.

Core Features | Part 13

- The use of a rootkit in SeroXen enhances its stealth capabilities and makes it more difficult for attackers to detect and remove the software. This is particularly useful in situations where the attacker has gained unauthorized access to a remote system and is attempting to maintain persistent access.
- In conclusion, SeroXen's rootkit feature makes it difficult to detect and remove the software from a remote system, enhancing its stealth capabilities and making it more difficult for attackers to maintain persistent access.

Core Features | Conclusion

- SeroXen is a powerful remote access tool that offers a wide range of features to help users manage and control remote systems. The tool offers a variety of capabilities, including Remote Desktop, HVNC, Show Messagebox, Send to Website, Update SeroXen Client File, Change Client Identification Tag, Remove Offline Client, Reconnect, and Uninstall SeroXen Client File. These features can be useful for troubleshooting, system administration, and maintaining system performance. However, it is important to note that some features, such as HVNC, are strictly for pentesting only and should not be used for any illegal purposes.

Plugin Features | Part 1

- C# Unrestricted Execution Based Plugin System:
- SeroXen is a remote access tool that offers a wide range of features to help users manage and control remote systems. One of the most powerful features of SeroXen is its C# unrestricted execution based plugin system. This system allows users to execute code on both the server (SeroXen UI) and the client (remote computer) using plugins written in C#.
- The C# unrestricted execution based plugin system of SeroXen allows users to execute any C# code that C# can execute. This means that users can write plugins that can perform any action that is possible with C#, including accessing the file system, networking, and interacting with the user interface.

Plugin Features | Part 2

- Execution on Server:
- Plugins written for SeroXen can be executed on the server (SeroXen UI) to perform actions on the remote system. This allows users to perform actions on the UI. For example, a plugin could be written to automatically perform tasks on the UI, such as adding features to the UI or UI feature addons.
- Execution on Client:
- Plugins written for SeroXen can also be executed on the client (remote computer) to perform actions on the system. This allows users to perform actions on the remote system that are not possible through the SeroXen UI. For example, a plugin could be written to monitor system activity and send alerts to the user if suspicious activity is detected.

Plugin Features | Part 3

- Usefulness of the Plugin System:
- The plugin system of SeroXen is incredibly useful for a variety of reasons. First, it allows users to extend the functionality of the tool to perform custom actions that are not available in the core feature set. This allows users to tailor the tool to their specific needs and to perform actions that are unique to their environment.
- Second, the plugin system allows users to automate routine tasks and perform them more efficiently. For example, a plugin could be written to automatically backup important data on the remote system, reducing the need for manual backups.
- Finally, the plugin system allows users to perform actions on the remote system that are not possible through the SeroXen UI. This allows users to monitor system activity, detect potential security threats, and perform other actions that would otherwise be impossible.

Plugin Features | Part 4

- Execution of Plugins via Remote Execute:
- Plugins written for SeroXen can be executed via the Remote Execute feature. Remote Execute is a feature that allows users to execute commands on the remote system. This feature can be used to execute plugins on the remote system.
- To execute a plugin via Remote Execute, the user must first upload the plugin to the remote system. This can be done using the Remote Execution feature of SeroXen. This allows the user to perform actions on the remote system without needing to have direct access to the system.

Plugin Features | Part 5

- Execution of Plugins via Autoexec Folder:
- Plugins can also be executed automatically when SeroXen is started by placing them in the Autoexec folder in the SeroXen directory. The Autoexec folder contains plugins that are executed automatically when SeroXen starts up. This allows users to automate routine tasks and perform them more efficiently.
- However, to enable the Auto Execute feature for a plugin, the plugin must be signed with a certificate issued by the SeroXen team. The Auto Execute DLL's feature must also be enabled in the SeroXen settings tab. This is done to prevent unauthorized plugins from being executed automatically and to ensure the security of the main and remote system.

Plugin Features | Conclusion

- Conclusion:
- The execution of plugins via Remote Execute and the Autoexec folder in the SeroXen directory is a powerful feature that allows users to extend the functionality of the tool and automate routine tasks. However, the Auto Execute DLL's feature must be enabled and the plugin must be signed with a certificate issued by the SeroXen team to ensure the security of the remote system. This feature is an essential tool for managing and controlling remote systems and is a valuable addition to any system administrator's toolkit.
- The C# unrestricted execution based plugin system of SeroXen is an incredibly powerful feature that allows users to execute code on both the server (SeroXen UI) and the client (remote computer) using plugins written in C#. This system allows users to extend the functionality of the tool, automate routine tasks, and perform actions that are not possible through the SeroXen UI. It is an essential tool for managing and controlling remote systems and is a valuable addition to any system administrator's toolkit.

How do I setup SeroXen? | Part 1

- SeroXen is a remote administration tool that is used for controlling a remote computer. In order to use SeroXen, the user needs to port forward the software to be able to access the remote computer. Port forwarding is a necessary step to be able to communicate with the remote computer over the internet.
- Port forwarding is the process of opening a specific port on a router or firewall so that data can flow through that port to the destination computer. This is necessary because most routers and firewalls are designed to block incoming connections by default. By port forwarding, the user can tell the router or firewall to allow incoming connections on a specific port, which is required for SeroXen to work properly.

How do I setup SeroXen? | Part 2

- To port forward SeroXen, the user must follow these steps:
- Determine the IP address of the computer running SeroXen. This can be found by typing "ipconfig" into the command prompt and looking for the "IPv4 Address" under the appropriate network adapter.
- Log into the router's admin interface. This can usually be done by typing the router's IP address into a web browser.
- Find the "Port Forwarding" or "Virtual Server" section of the router's settings. This may be located under "Advanced Settings" or a similar section.

How do I setup SeroXen? | Part 3

- Create a new port forwarding rule. The user will need to enter the following information:
 - The name of the rule (e.g. SeroXen)
 - The port number used by SeroXen (default is 4782)
 - The IP address of the computer running SeroXen
 - The protocol used by SeroXen (TCP)
 - Save the port forwarding rule and exit the router's admin interface.

How do I setup SeroXen? | Conclusion

- Configure SeroXen to use the port number that was forwarded. This can be done in the "Settings" tab of the SeroXen UI.
- Test the port forwarding by attempting to connect to the SeroXen client from a remote computer.
- It's important to note that port forwarding can potentially expose the computer running SeroXen to security risks. It's recommended that the user takes appropriate measures to secure their network and computer, such as enabling a firewall, using strong passwords, and regularly updating their antivirus software. Additionally, it's important to follow all applicable laws and regulations when using SeroXen.