After reading “Linux Rootkit,” located in the topic Resources, what features of this application qualify it is a rootkit? The author says that “this toolkit is for fun, not evil.” Explain your thoughts on this statement.

Hello Class,

As Warren had mentioned, I did not find the resource titled ‘Linux Rootkit”. A rootkit is a program or a collection of malicious software tools that give a threat actor remote access to and control over a computer or other system. Some features of an application that qualify it as a rootkit include:

Provision of remote access. Rootkits often provide the ability for an attacker to remotely control the compromised system. Hiding files, processes, and network activity. Rootkits are designed to conceal their presence and activities from detection by antivirus software and system administrators. Privileged access. Rootkits typically gain administrative or root-level access to a computer, allowing them to perform actions that are not normally permitted.

Regarding the statement "this toolkit is for fun, not evil," it is important to note that rootkits are inherently malicious in nature. They are designed to compromise the security and integrity of a system, often for malicious purposes such as unauthorized access, data theft, or control of the compromised system. Therefore, any application that qualifies as a rootkit cannot be considered "for fun" as it poses a serious threat to the security and privacy of users.

References:

What is a rootkit? (n.d.). SearchSecurity. https://www.techtarget.com/searchsecurity/definition/rootkit

What is Rootkit? Attack Definition & Examples | CrowdStrike. (2021, September 30). Crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/malware/rootkits/

Wikipedia Contributors. (2019, August 2). Rootkit. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Rootkit