8.3.5 Exploit Systems to Maintain Access Facts

Hackers like to keep access to the systems they have gained admin or root access to. They also work hard to keep other hackers out of the system. At the admin or root level, they have the ability to download or upload anything, capture and manipulate data, and configure applications and services. They can also use the system to exploit other systems.

The following table lists a few ways a hacker can maintain access:

Method	Description
Path interception	When an executable such as an app, service, or process is started, the system looks for a path for the file that runs it. There is no problem if the path is written within quotation marks and has no spaces. However, if the path name doesn't have quotation marks around it and there are spaces in the path name, there is an opportunity for a hacker to add a path that routes to a malicious file. Executables called on a regular basis can provide continued access to a system. Executables started by a higher privileged process can give the hacker elevated privileges, allowing the hacker to create a new user in the system with administrator rights providing ongoing system access. Here is an example: Trusted Path: Path to executable: “c:\programfiles\subdirectory\programname.exe” Exploitable Path: Unquoted path with spaces: c:\program files\sub directory\program name.exe
Writable services	Another way to exploit a service is to search for admin level accounts that have services that are writable. Services with weak permissions allow anyone to alter the execution of the service. This may include creating a new admin user account that gives the hacker rights to do whatever the admin account can do.
Unsecure file and folder permissions	Older versions of Windows allow administrators to access the files and folders of any non-admin user. This can lead to DLL hijacking and malicious file installations on a non-admin targeted user.

The following table describes additional ways a hacker can establish continued access to the systems they hack.

Method	Description
Backdoors	When hackers gain access to a system, often they establish a way to get back into it again later. This is referred to as a backdoor. Typically, a hacker will install a rootkit, Trojan horse, or a remote access Trojan (RAT). Rootkits have access at the operating system level and Trojans have access at the application level. As previously discussed, a hacker may create a new user to obtain access.
Crackers	Crackers are software programs that crack code and passwords to gain unauthorized access to a system. There are many methods and tools available for this approach such as dictionary, brute force, and rainbow attacks.
Spyware	Spyware is malware that works by stealth to capture information and sends it to a hacker to gain access. Spyware can be keystroke logging, activity tracking, screen captures, or file operations. Spyware can be unintentionally installed by a user through normal web activity and it is often undetected. Hackers may install backdoors into the system to maintain access to the spyware.
Scheduled Tasks	When processing task files, Windows Task Scheduler has a vulnerability in its validation of the files. It has a default configuration that allows regular users to write task files. An attacker can modify a task file to execute malicious commands. This method can be used to escalate privileges, maintain access, perform remote execution, and implement malicious programs at system startup.