Report “Null Session”

Null Sessions are anonymous connections to Windows systems without authentication. They are often exploited to obtain sensitive information across a target network, using empty SMB (Server Message Block) sessions, to access shared resources on the network.

Vulnerable OS:
-Windows XP
-Windows 2000
-Windows NT
-Windows Server

Currently these operating systems are not used at enterprise level as they are obsolete and no longer supported by Microsoft, but in some circumstances, especially in the PA, they are still in circulation.

Risk & Mitigation

Risk

The risk regarding Null Sessions is very high in proportion to the potential for damage that can be caused. In fact, an attacker, by exploiting these vulnerabilities, can gain possession of sensitive and exclusive-use files, which can compromise both the company and the person.

Mitigation

-Disabling Null Session:

In this case we have two options; the first consists in deactivating these sessions while the second in inserting policies regarding sharing and authentication.

This type of intervention is very effective but requires specific knowledge of the network in question and the processes that are created to carry out authentication.

-Network control:

By ensuring we don't share important files and managing access to shares, we can significantly reduce the impact of an attack.

It is a type of intervention that requires attention from all users of the network, making it easier to apply but much less to maintain as human error can occur at any time.

-Network update:

By keeping systems updated through patches and upgrades, you can avoid flaws due to problems that the developer himself has already solved.

In this case the difficulty can vary from situation to situation, making the process easier in the latest generation networks. On older and no longer supported systems the process can be more complicated.

-Monitoring:

By implementing monitoring systems, both for access and sharing, the risk of exploits can be practically reduced to zero.

This activity is certainly more expensive than the previous ones but it is the one that guarantees greater privacy and control, determining a solid security basis in the network.

COSTS:

The costs relating to the mitigation processes listed above vary greatly between the types of operations.
Generally, adequate training of IT staff guarantees a good starting point in achieving the objective. In this case the costs vary based on the type of training you want to undertake, but usually a good level networking certification costs around €600/700 including lessons.
However, if you also want to add monitoring systems, the price increases for the additional services. Several companies offer systems that guarantee advanced operation and security, the choice may depend on the systems used. On average, however, for a network monitoring service, which includes Network Management software, various devices and related training, costs start from around €2000. The price can then increase by adding additional licenses and deploying new devices.

In conclusion:

Carrying out this type of operation can be challenging initially, but in this era, cybersecurity is a variable that can mean everything, regardless of the size of the company in question. A single error can be "fatal" both at an image and economic level and it is therefore highly recommended to implement network security systems as much as possible.
Finally, raising awareness on the topic and involving staff turns out to be one of the least expensive and most efficient weapons available.