Exploitation of Remote Services, Technique T1210 - Enterprise

Archived: 2026-04-05 15:29:09 UTC

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

An adversary may need to determine if the remote system is in a vulnerable state, which may be done through Network Service Discovery or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources.

There are several well-known vulnerabilities that exist in common services such as SMB[1] and RDP[2] as well as applications that may be used within internal networks such as MySQL[3] and web server services.[4][5] Additionally, there have been a number of vulnerabilities in VMware vCenter installations, which may enable threat actors to move laterally from the compromised vCenter server to virtual machines or even to ESXi hypervisors.[6]

Depending on the permissions level of the vulnerable remote service an adversary may achieve Exploitation for Privilege Escalation as a result of lateral movement exploitation as well.

Source: https://attack.mitre.org/techniques/T1210/