CAPEC-555: Remote Services with Stolen Credentials (Version 3.9)

Archived: 2026-04-06 01:50:09 UTC

Attack Pattern ID: 555 **Abstraction: Standard**		

Description

This pattern of attack involves an adversary that uses stolen credentials to leverage remote services such as RDP, telnet, SSH, and VNC to log into a system. Once access is gained, any number of malicious activities could be performed.

Typical Severity

Very High

Relationships

This table shows the other attack patterns and high level categories that are related to this attack pattern. These relationships are defined as ChildOf and ParentOf, and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as CanFollow, PeerOf, and CanAlsoBe are defined to show similar attack patterns that the user may want to explore.

Nature	Type
ChildOf	Meta Attack Pattern - A meta level attack pattern in CAPEC is a decidedly abstract characterization of a specific methodology or techn
CanPrecede	Meta Attack Pattern - A meta level attack pattern in CAPEC is a decidedly abstract characterization of a specific methodology or techn
CanPrecede	Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific techni

This table shows the views that this attack pattern belongs to and top level categories within that view.

View Name	Top Level Categories
Domains of Attack	Software
Mechanisms of Attack	Subvert Access Control

Mitigations

Disable RDP, telnet, SSH and enable firewall rules to block such traffic. Limit users and accounts that have remote interactive login access. Remove the Local Administrators group from the list of groups allowed to login through RDP. Limit remote user permissions. Use remote desktop gateways and multifactor authentication for remote logins.

Example Instances

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS). There are other implementations and third-party tools that provide graphical access Remote Services similar to RDS. Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials.
Windows Remote Management (WinRM) is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, modify services). It may be called with the winrm command or by any number of programs such as PowerShell.

Taxonomy Mappings

CAPEC mappings to ATT&CK techniques leverage an inheritance model to streamline and minimize direct CAPEC/ATT&CK mappings. Inheritance of a mapping is indicated by text stating that the parent CAPEC has relevant ATT&CK mappings. Note that the ATT&CK Enterprise Framework does not use an inheritance model as part of the mapping to CAPEC.

Relevant to the ATT&CK taxonomy mapping (also see parent)

Entry ID	Entry Name
1021	Remote Services
1114.002	Email Collection:Remote Email Collection
1133	External Remote Services

Content History

Submissions		
Submission Date	**Submitter**	**Organization**
2015-11-09 (Version 2.7)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**
2018-07-31 (Version 2.12)	CAPEC Content Team	The MITRE Corporation
	Updated Description Summary, Examples-Instances, References, Related_Weaknesses, Typical_Severity	
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated @Abstraction, Related_Attack_Patterns, Related_Weaknesses, Taxonomy_Mappings	
2022-09-29 (Version 3.8)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	

More information is available — Please select a different filter.
