Lateral Movement, Tactic TA0008 - Enterprise

Archived: 2026-04-05 14:55:20 UTC

T1210 Exploitation of Remote Services 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. T1534 Internal Spearphishing After they already have access to accounts or systems within the environment, adversaries may use internal spearphishing to gain access to additional information or compromise other users within the same organization. Internal spearphishing is multi-staged campaign where a legitimate account is initially compromised either by controlling the user's device or by compromising the account credentials of the user. Adversaries may then attempt to take advantage of the trusted internal account to increase the likelihood of tricking more victims into falling for phish attempts, often incorporating Impersonation. T1570 Lateral Tool Transfer Adversaries may transfer tools or other files between systems in a compromised environment. Once brought into the victim environment (i.e., Ingress Tool Transfer) files may then be copied from one system to another to stage adversary tools or other files over the course of an operation. T1563 Remote Service Session Hijacking Adversaries may take control of preexisting sessions with remote services to move laterally in an environment. Users may use valid credentials to log into a service specifically designed to accept remote connections, such as telnet, SSH, and RDP. When a user logs into a service, a session will be established that will allow them to maintain a continuous interaction with that service. .001 SSH Hijacking Adversaries may hijack a legitimate user's SSH session to move laterally within an environment. Secure Shell (SSH) is a standard means of remote access on Linux and macOS systems. It allows a user to connect to another system via an encrypted tunnel, commonly authenticating through a password, certificate or the use of an asymmetric encryption key pair. .002 RDP Hijacking Adversaries may hijack a legitimate user’s remote desktop session to move laterally within an environment. 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). T1021 Remote Services Adversaries may use Valid Accounts to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. .001 Remote Desktop Protocol Adversaries may use Valid Accounts to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user. .002 SMB/Windows Admin Shares Adversaries may use Valid Accounts to interact with a remote network share using Server Message Block (SMB). The adversary may then perform actions as the logged-on user. .003 Distributed Component Object Model Adversaries may use Valid Accounts to interact with remote machines by taking advantage of Distributed Component Object Model (DCOM). The adversary may then perform actions as the logged-on user. .004 SSH Adversaries may use Valid Accounts to log into remote machines using Secure Shell (SSH). The adversary may then perform actions as the logged-on user. .005 VNC Adversaries may use Valid Accounts to remotely control machines using Virtual Network Computing (VNC). VNC is a platform-independent desktop sharing system that uses the RFB ("remote framebuffer") protocol to enable users to remotely control another computer’s display by relaying the screen, mouse, and keyboard inputs over the network. .006 Windows Remote Management

Adversaries may use Valid Accounts to interact with remote systems using Windows Remote Management (WinRM). The adversary may then perform actions as the logged-on user. .007 Cloud Services Adversaries may log into accessible cloud services within a compromised environment using Valid Accounts that are synchronized with or federated to on-premises user identities. The adversary may then perform management actions or access cloud-hosted resources as the logged-on user. .008 Direct Cloud VM Connections Adversaries may leverage Valid Accounts to log directly into accessible cloud hosted compute infrastructure through cloud native methods. Many cloud providers offer interactive connections to virtual infrastructure that can be accessed through the Cloud API, such as Azure Serial Console, AWS EC2 Instance Connect, and AWS System Manager.. T1091 Replication Through Removable Media Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself. T1072 Software Deployment Tools Adversaries may gain access to and use centralized software suites installed within an enterprise to execute commands and move laterally through the network. Configuration management and software deployment applications may be used in an enterprise network or cloud environment for routine administration purposes. These systems may also be integrated into CI/CD pipelines. Examples of such solutions include: SCCM, HBSS, Altiris, AWS Systems Manager, Microsoft Intune, Azure Arc, and GCP Deployment Manager. T1080 Taint Shared Content Adversaries may deliver payloads to remote systems by adding content to shared storage locations, such as network drives or internal code repositories. Content stored on network drives or in other shared locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files. Once a user opens the shared tainted content, the malicious portion can be executed to run the adversary's code on a remote system. Adversaries may use tainted shared content to move laterally. T1550 Use Alternate Authentication Material Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls. .001 Application Access Token Adversaries may use stolen application access tokens to bypass the typical authentication process and access restricted accounts, information, or services on remote systems. These tokens are typically stolen from users or services and used in lieu of login credentials. .002 Pass the Hash Adversaries may "pass the hash" using stolen password hashes to move laterally within an environment, bypassing normal system access controls. Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. .003 Pass the Ticket Adversaries may "pass the ticket" using stolen Kerberos tickets to move laterally within an environment, bypassing normal system access controls. Pass the ticket (PtT) is a method of authenticating to a system using Kerberos tickets without having access to an account's password. Kerberos authentication can be used as the first step to lateral movement to a remote system. .004 Web Session Cookie Adversaries can use stolen session cookies to authenticate to web applications and services. This technique bypasses some multi-factor authentication protocols since the session is already authenticated.
