# TTP Detail – T1098.004

## TTP Information

Name: SSH Authorized Keys

Description: Adversaries may modify the SSH <code>authorized\_keys</code> file to maintain persistence on a victim host. Linux distributions, macOS, and ESXi hypervisors commonly use key-based authentication to secure the authentication process of SSH sessions for remote management. The <code>authorized\_keys</code> file in SSH specifies the SSH keys that can be used for logging into the user account for which the file is configured. This file is usually found in the user's home directory under <code>&lt;user-home&gt;/.ssh/authorized\_keys</code> (or, on ESXi, `/etc/ssh/keys-<username>/authorized\_keys`).(Citation: SSH Authorized Keys) Users may edit the system’s SSH config file to modify the directives `PubkeyAuthentication` and `RSAAuthentication` to the value `yes` to ensure public key and RSA authentication are enabled, as well as modify the directive `PermitRootLogin` to the value `yes` to enable root authentication via SSH.(Citation: Broadcom ESXi SSH) The SSH config file is usually located under <code>/etc/ssh/sshd\_config</code>.

Adversaries may modify SSH <code>authorized\_keys</code> files directly with scripts or shell commands to add their own adversary-supplied public keys. In cloud environments, adversaries may be able to modify the SSH authorized\_keys file of a particular virtual machine via the command line interface or rest API. For example, by using the Google Cloud CLI’s “add-metadata” command an adversary may add SSH keys to a user account.(Citation: Google Cloud Add Metadata)(Citation: Google Cloud Privilege Escalation) Similarly, in Azure, an adversary may update the authorized\_keys file of a virtual machine via a PATCH request to the API.(Citation: Azure Update Virtual Machines) This ensures that an adversary possessing the corresponding private key may log in as an existing user via SSH.(Citation: Venafi SSH Key Abuse)(Citation: Cybereason Linux Exim Worm) It may also lead to privilege escalation where the virtual machine or instance has distinct permissions from the requesting user.

Where authorized\_keys files are modified via cloud APIs or command line interfaces, an adversary may achieve privilege escalation on the target virtual machine if they add a key to a higher-privileged user.

SSH keys can also be added to accounts on network devices, such as with the `ip ssh pubkey-chain` [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) command.(Citation: cisco\_ip\_ssh\_pubkey\_ch\_cmd)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation

## Malware

* Bundlore
* Skidmap
* XCSSET

## APTs (Intrusion Sets)

* Earth Lusca
* Salt Typhoon
* TeamTNT