Template - Account enumeration reconnaissance

Link to alert

**Description**

In account enumeration reconnaissance, an attacker uses a dictionary with thousands of usernames, or tools such as KrbGuess in an attempt to guess user names in the domain.

**Classification**: Incident

**How to investigate**

[Microsoft Defender for Identity reconnaissance phase security alerts | Microsoft Docs](https://docs.microsoft.com/en-us/defender-for-identity/reconnaissance-alerts)

**Alert detail**

Account names:

DC:

First activity:

Last activity:

External Computer name:

IP address of External Computer:

Severity: Medium

**Remediation**

Contain the source computer.

* Find the tool that performed the attack and remove it.
* Look for users who were logged on around the same time as the activity occurred, as these users may also be compromised.
* Reset their passwords and enable MFA or, if you've configured the relevant high-risk user policies in Azure Active Directory Identity Protection, you can use the **Confirm user compromised** action in the Cloud App Security portal.

Enforce Complex and long passwords in the organization.

***NB: PROVIDE A SCREESNHOT OF THE WORK DONE***