Open Infrastructure - Task #7546

VM Security based on LDAP accounts

12/31/2019 07:40 PM - Moris Jones

Status:	Rejected	**Start date:**	12/31/2019
Priority:	Normal	**Due date:**	
Assignee:	Mondi Ravi	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
PM Check date:			

Description

Access to VM administration tools should be secured to the same level or higher as root access to the VM itself.

Currently the VM dashboard uses a shared login with redmine.

Admin systems and communication systems should not have a shared login system, this is a single point of failure.

More details here:

https://chat.ungleich.ch/ungleich/channels/remote-root-exploits-in-ungleich-shared-login-to-different-sys

History

#1 - 01/01/2020 04:53 PM - Nico Schottelius

- Project changed from Digitale Bildung ungleich to Open Infrastructure

- Status changed from New to In Progress

#2 - 01/01/2020 05:05 PM - Nico Schottelius

- Subject changed from VM Security to VM Security based on LDAP accounts

Clarification 1: "shared login"

We use LDAP servers as a backend to redmine and django (the dashboard). Both systems originally had their own user databases (and passwords), but both have been reconfigured to use the LDAP backend.

Attack vector 1: hacked systems

- If redmine is hacked, no passwords/access leak, as the data is not in redmine

Attack vector 2: django is hacked

If the django application is hacked, the attacker gains direct access to the VM - nothing changed here.

Attack vector 3: ldap / indirect hack

- If either redmine or django don't imply rate limiting, brute force attacks are possible
  - This needs to be verified for both systems
  - Mondi: can you checkout & if necessary fix on django?
  - Timothee: can you checkout & if necessary fix on redmine?
- Access to the LDAP servers
  - The LDAP servers should only be reachable from dedicated applications
  - Timothee, can you verify/update the nftables on ldap1 and ldap2 that access to the ldap ports is only possible from dynamicweb-production.u and redmine.u?

Further security improvements

Moris suggested to disallow VM termination in the web interface and only allow to terminate the VM using ssh keys. Statement from our side to this:

- It's a good idea, but not feasible for many customers
- There could be an optional "dangerous methods only via SSH" checkbox on the web
  - If checked, VMs can only be terminated via SSH

    - If checked, it cannot be unchecked from the web, but only via SSH
    - Opt-in needed, because default users won't
- If somebody (Moris?) provides code/patches to dynamicweb, we are happy to accept it
- However the SSH based restrictions is not high prio in the development queue

#3 - 01/01/2020 05:05 PM - Nico Schottelius

- Assignee changed from Nico Schottelius to Mondi Ravi

- Moris, thanks for reporting.
- Mondi, can you start with your tasks and handover to Timothee when done?

#4 - 01/01/2020 05:49 PM - Mondi Ravi

We don't have any rate limiting to any of the apis that we have so far.

I think rate limiting would primarily be needed for the user login/signup attempts, but not limited to them only.

We could also add captchas.

#5 - 01/02/2024 02:06 PM - Nico Schottelius

- Status changed from In Progress to Rejected