Windows domain accounts on Linux

Closing an ssh key authentication security gap

Scott Nolin
31 May 2018
Introduction

At SSEC we use Windows domain accounts and groups to control access and permissions for both windows and Linux systems.

This works well, but Linux systems with ssh key authentication required some thought and a little scripting.
The easy flow chart!

User Logs In

Pass AD Authentication?

User in "users" LOCAL group?

User in "unixadmins" AD group?

ALLOW Access

DENY Access
If SSH Key authentication is allowed

User Logs In

SSH Key

NO

Pass AD Authentication?

NO

User in "users" LOCAL group?

NO

User in "unixadmins" AD group?

NO

DENY Access

YES

ALLOW Access

YES

YES

NO

NO
SSH Key Auth = no AD Auth

- Disabled user account?
- Expired user account?
- Password Change required?

Come on in!
Our Scheme: Use AD Groups

User Logs In

Pass AD Authentication?

YES

SSH Key

NO

In “expiredusers” AD group?

NO

In “disabledusers” AD group?

NO

In “users” LOCAL group?

NO

User in “unixadmins” AD group?

NO

YES

DENY Access

ALLOW Access

NO

NO

NO

NO

NO

YES

YES

6/2/2018 University of Wisconsin–Madison
Linux Client Details

- Samba-winbind clients (SSSD would be essentially the same)
- PAM access.conf to allow groups
  - : disabledusers : ALL
  - : expiredusers : ALL
  + : unixadmins : ALL
  + : users : ALL
  - : ALL : ALL

- Users is a local group, others are domain groups.
  - We have many hosts, avoided creating a domain users group for each host.
Windows AD Script Details

• Three scripts
  1. Find all expired user accounts and create ‘expiredusers’ group.
  2. Find all disabled users and create ‘disabledusers’ group.
  3. Process disabled user accounts
     • Remove from all groups (except domain users)
     • Move to a special OU.

• Actions are logged
• Account expiry is automated, a human has to disable an account. Expired account are routinely enabled, so don’t strip groups.
Limitations, issues, etc

• It is easy to conflate ‘disabledusers’ with Windows disabled user accounts.
  • If you put a user in ‘disabledusers’ group – the account isn’t disabled. You’ve blocked ssh access, that’s all. ‘disabled_ssh’ may be a better group name.

• Scripts are run periodically, so access is not blocked instantly.
• Linux clients may cache group membership for a while.
• We do not address expired passwords and ssh key authentication