Homework 4
LDAP

cwang, hslin

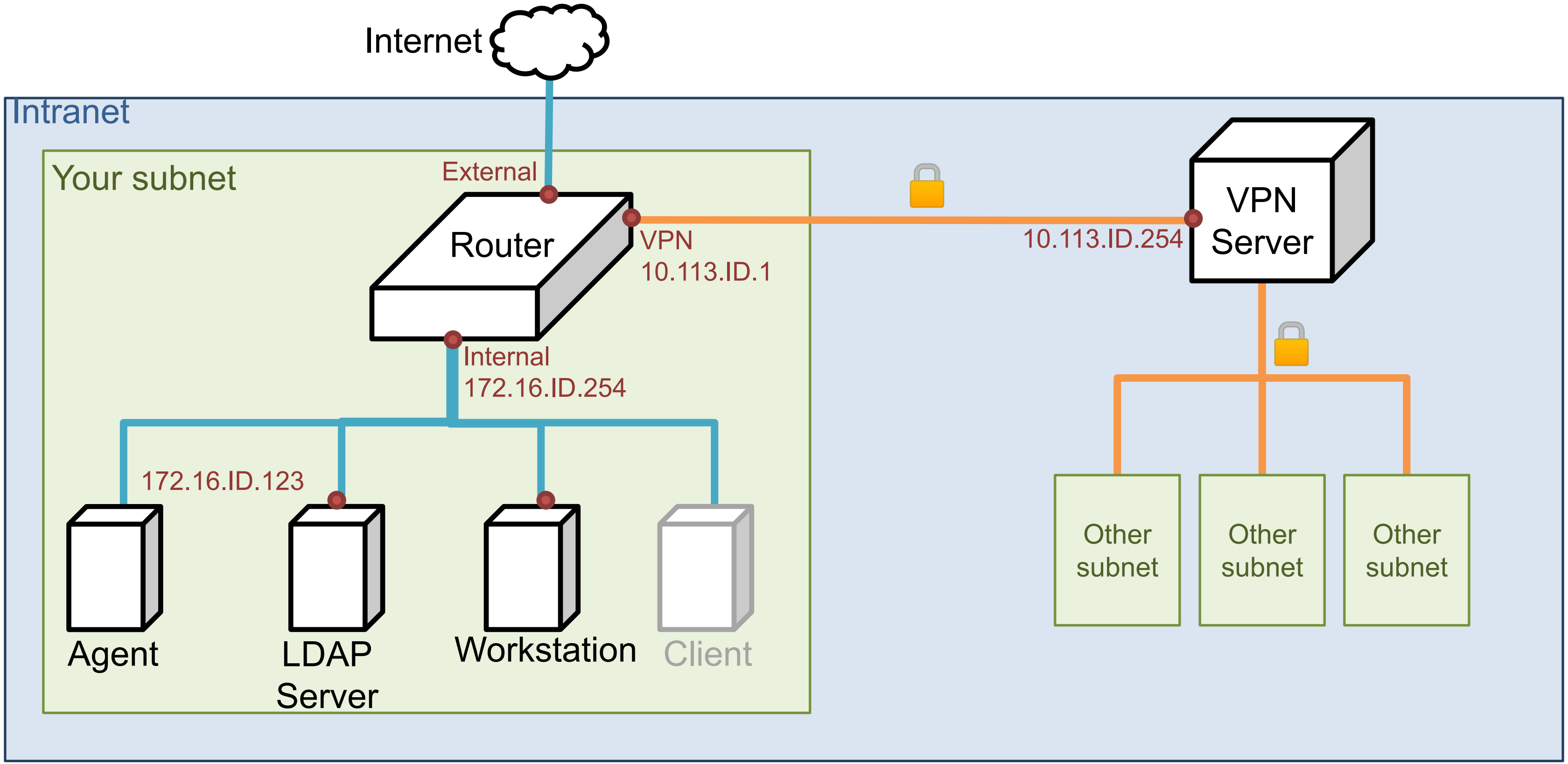
國立陽明交通大學資工系資訊中心

Computer Center of Department of Computer Science, NYCU

Purposes

- Build a basic LDAP service
- Understand how to…
  - configure LDAP server
  - manage LDAP data using LDIF
  - auth and permission control on Unix client with LDAP server
  - understand and use Ansible

Overview - Architecture



Overview (cont.)

- A simple LDAP server
  - LDAP client
- One or more Workstations
  - LDAP client

Requirements

- LDAP Server
  - IP: 172.16.ID.y/24 with static DHCP, where y is arbitary.
  - Hostname: ldap.{ID}.nasa. (5%)
  - Base DN: dc=<ID>, dc=nasa
  - LDAP over TLS (StartTLS) and force TLS search (8%)
    - Not LDAPS
    - Use self-signed certificate
    - Add your CA certificate to DNS TXT Record
      - cert => `base64 cacert.pem`

Requirements

- Workstation
  - IP: 172.16.ID.y/24 with static DHCP, where y is arbitary
  - Hostname: workstation.{ID}.nasa.   (5%)
  - You need use Ansible to build workstation

Requirements

We need two user group in LDAP:

- ta group
  - can login (ssh) into LDAP server and any workstations (14%)
  - can use sudo for any command (13%)
    - ex. `sudo adduser`
- stu group
  - can login (ssh) into workstations, doesn’t login into LDAP server
  - only use sudo for `cat` command
- You need use “LDAP” to implement above requirements
- TA will add any name user into these group

Requirements

Add an user with DN “uid=ta1,ou=People,<Base DN>”

- This user under ta group, use ta group permission
- Allow this user to connect via SSH with both ssh public key and password
  - uid: ta1
  - uid number: 10001
  - public key: <ta’s public key>   # below page
  - user password: <your TA_PASSWORD>
    - user password need hash

Requirements

TA's public key: https://nasa.cs.nctu.edu.tw/na/2022/id_rsa.pub

- Fingerprint:

```
$ ssh-keygen -l -f id_rsa.pub
3072 SHA256:KMCo/a1eZvhhmtYi4uoPWoBeglDGSJxhH0IXvAxPXBc 2022-na-hw4 (RSA)
```

Requirements

Add another user with DN “uid=stu<ID>,ou=People,<Base DN>”

- This user under stu group, use stu group permission
- Allow this user to connect via SSH with both ssh key and password
    - uid: stu<ID>
        - e.g. stu1, stu55
    - uid number: 20000 + <ID>
        - e.g. 20001, 20055
    - user password: <your TA_PASSWORD>

Requirements

- Configure LDAP Client on every machine
  - Configure LDAP for login (ssh) authentication
    - can use password or public key login
  - When you add a user into LDAP, this user can login on any workstation or LDAP Server
  - Login permissions at Page 7

Requirements

- Set proper LDAP access control
  - Allow users to modify their own userPassword and ssh public key (8%)
    - Set other attributes as read-only (8%)
  - Allow users to search all user data except other users' password (8%)
    - i.e., users can only search their own password
- Set password policy for each user (ta, stu … etc)
  - userPassword can't same as previous when change password (8%)
    - But can set password as previous two time used
    - You need implement this by LDAP way
    - Hint & Require : ppolicy overlay

Requirements

- Ansible
  - Build all workstation requirements
  - Implement ansible playbook, role, template, task and handler. (10%)
    - Ref: Ansible Best Practice

Submission - Online Judge

- Your work will be tested by our online judge system
  - Submit a judge request when you are ready.
  - You can submit request multiple times. However, the score of the last submission instead of the submission with the highest score, will be taken.
  - Late submissions are not accepted.
  - Please check your score at OJ after judge completed.
- Scoring starts at : 2022/5/16 (Thur.) 00:00
  - The cool-down time is 30 minutes
- Deadline: 2022/6/9 (Thur.) 23:59

Submission - Online Demo

- Scoring Structure
  - Online Judge 50% + Demo 50%
- Ta will ask some questions about your architecture in Demo Time
  - Ex: How do you handle group permission issue
- Online Demo time and detail will release later on E3

Submission - Online Demo

- Online Demo
  - No manual involve for install, setting
  - You need prepare a clean, installed VM before demo (from official image)
  - Run your ansible file on VM to build a workstation
    - ldapsearch success (5%)
    - Explain your ansible file (5%)
    - Workstation domain and IP specify by TA
    - TIMEOUT 5 MINUTES
  - Use `ldapadd` to add user and set user group (3%)
  - Use `ldapmodify` to modify user
  - Check login and sudo permissions
    - For LDAP Server and workstation
    - You can’t edit any configuration on LDAP Server

Help

- Due to the pandemic, NO TA office hours
  - Please ask your questions online
- Questions about this homework.
  - Make sure you have studied through lecture slides and the HW spec.
  - Clarify your problems and search it to find out solutions first.
  - Ask them on https://groups.google.com/g/nctunasa .
    - Be sure to include all the information you think others would need

Good Luck!