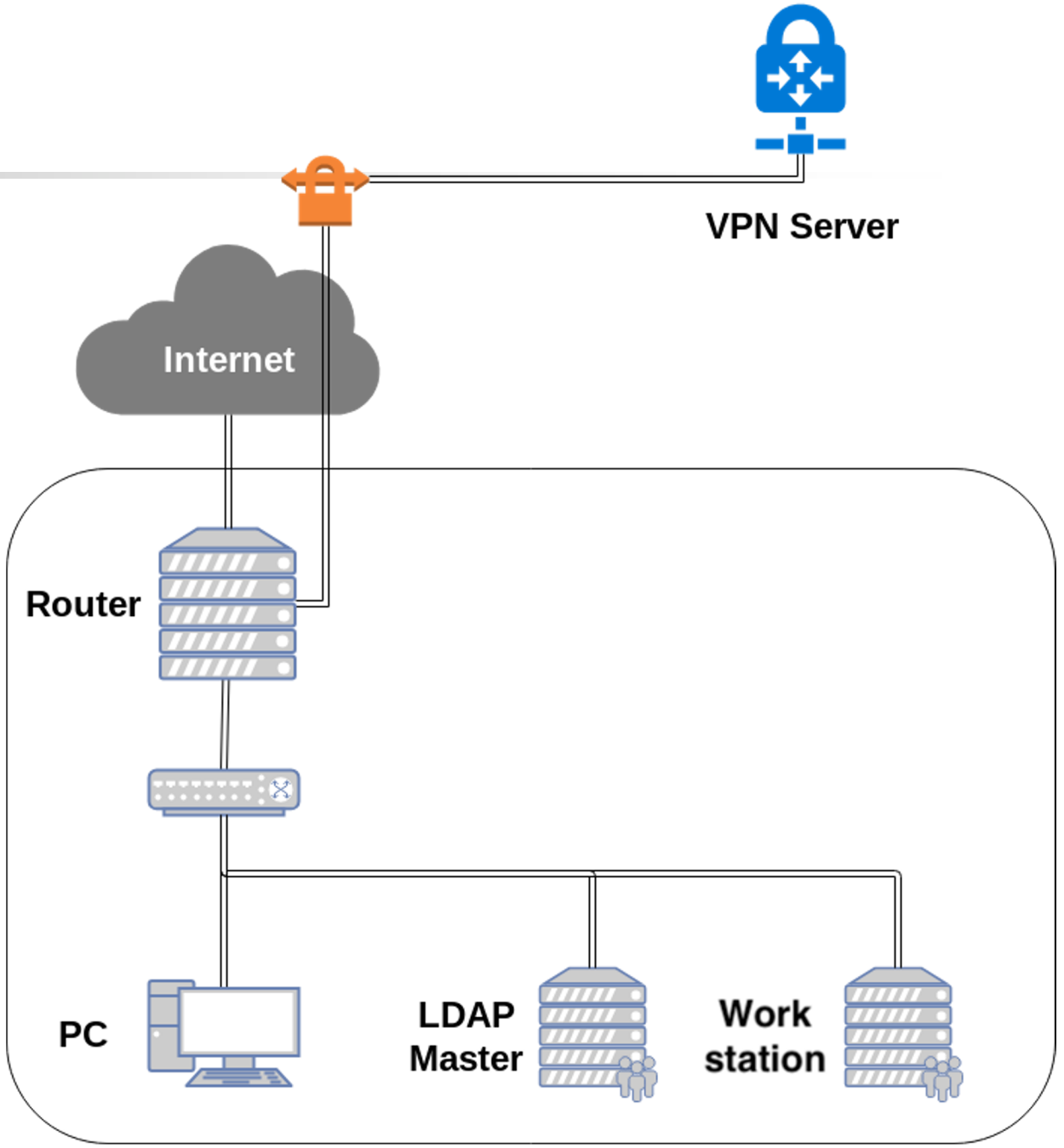
Network Administration HW4

yysung

Purposes

- Build a standalone LDAP service
- Understand how to define LDAP schema from scratch
- Understand how to manage LDAP datas using LDIF
- Understand how to integrate other applications with LDAP

Overview



Overview (Cont.)

- One LDAP master server
  - Providing LDAP service
  - Connecting into your intranet
  - LDAP Client
- One Workstation
  - SNMP Agent
  - Connecting into your intranet
  - LDAP Client

Requirements (1/10)

- LDAP master
  - IP: 10.113.ID.y/24 with static DHCP
  - Hostname: ldap1.{student_ID}.nasa.
  - Base DN: dc=<student-id>,dc=nasa
  - StartTLS on LDAP service
    - Not LDAPS
    - Use self-signed certificate
    - Add TXT Record

      cert => `base64 cacert.pem`
  - Support SASL
    - Store hashed password into each DN's userPassword

Requirements (2/10)

- Custom objectClass "ludouCredit"
  - attributeType "ludoucredit"
- ludoucredit should be an integer.
- ludoucredit can be compared with some constant integer. (Ordering Matching Rules)

- Everyone can read each other's ludoucredit, but only cn=TA and your manager account can modify other's ludoucredit.

Requirements (3/10)

- LDAP master, Workstation
  - Users can login with LDAP posixAccount
    - At least, login via SSH should be worked
  - Users can execute passwd to change their own password
  - Use attribute "uid" as username

- Specific user "cn=<student-id>,ou=People,<Base DN>"
  - uid: <student-id>
  - uidNumber: 3001
  - set your own password

Requirements (4/10)

- objectClass "publicKeyLogin"
  - attributeType "sshPublicKey"
- Specific DN "cn=TA,ou=People,<Base DN>"
  - objectClass: posixAccount, publicKeyLogin, ludouCredit
  - uid: TA
  - uidNumber: 3000
  - ludouCredit: 100
  - sshPublicKey: <TA's public key>
  - userPassword: your VPN private key (WG_KEY)
  - Should can login SSH with sshPublicKey and password
- Retrieve TA's public key here
  - https://nasa.cs.nctu.edu.tw/na/2020/ta_rsa.pub

Requirements (5/10)

- Specific DN "cn=taipeirioter,ou=People,<Base DN>"
  - objectClass: posixAccount, publicKeyLogin, ludouCredit
  - uid: taipeirioter
  - uidNumber: 4000
  - ludouCredit: 100
  - sshPublicKey: <TA's public key>
  - userPassword: your VPN private key (WG_KEY)
  - Should can login SSH with sshPublicKey and password

Requirements (6/10)

- Specs of ludouCredit about User Account and SSH Login:
  - If some users' ludoucredit > 0, they can login via SSH.
  - If some users' ludoucredit == 0, they can't login via SSH with TA's private key, but their account still exist on the system.
  - If some users' ludoucredit < 0, they can't login via SSH and their account will be disappeared on the LDAP master and Workstation. (i.e. id: user: no such user)

Requirements (7/10)

- Time-based One-Time Password (TOTP) (RFC6238)
  - Support TOTP on your LDAP master
  - time step = 30 seconds, digits = 6 (default value)
  - You may use https://github.com/openldap/openldap/tree/master/contrib/slapd-modules/passwd/totp overlay to implement.
- Specific DN "cn=totp,ou=People,<Base DN>"
  - objectClass: posixAccount, ludouCredit
  - uid: totp
  - userPassword: "{TOTP1}`printf ${WG_KEY} | base32`"
  - Can login via SSH or bind DN in LDAP with TOTP

Requirements (8/10)

- Enable ACL
  - Everyone (including anonymous) can read all data except userPassword
  - Authenticated users can write their own userPassword
  - LDAP Manager can write everyone's userPassword
  - LDAP Manager and TA can write everyone's ludoucredit, all the other users can't write anyone's ludoucredit

Requirements (9/10)

- Workstation
  - IP: 10.113.ID.y/24 with static DHCP
  - Hostname: ws1.{student_ID}.nasa.
  - Users can login via SSH with LDAP posixAccount
  - SNMP Agent (Net-SNMP)
- SNMP Agent on Workstation
  - Support v2c
  - Community "public"
    - Can access from intranet and your private network
    - Read Only
  - Community "private"
    - Can access only from 10.113.ID.0/24 and localhost
    - Read and Write

Requirements (10/10)

- {public, private} can read CPU 1 minute load
  - UCD-SNMP-MIB::laLoad.1
- {public, private} can read SNMPv2-MIB::sysName.0
- {private} can write SNMPv2-MIB::sysName.0
- Write an extend named "servicecheck"
  - Check the connection to tcp:10.113.ID.129:5566
  - If connected, nsExtendResult should be 0
  - If not connected, nsExtendResult should not be 0
  - You can test by command `snmpget -v2c -c public -Oqv localhost 'NET-SNMP-EXTEND-MIB::nsExtendResult."servicecheck"'`
  - Set your NET-SNMP-EXTEND-MIB::nsExtendCacheTime."servicecheck" <= 5

Firewall

- Open {LDAP, SSH} port on LDAP master to intranet
- Open {SNMP, SSH} port on Workstation to intranet
- Recall the rules.
  - By default, all connections from outside (include Intranet) to your subnet should be rejected.
  - By default, all services only trust the connections from your subnet.
  - SSH connections from anywhere to “Agent” are allowed.
  - ICMP connections from anywhere to anywhere are allowed.
- You won’t get any points for this part, but you will get some points down for the incorrect firewall setting.

Warning!!!

- Always SNAPSHOT or BACKUP YOUR SYSTEM before judging!!!
- Set {TA, taipeirioter, totp}'s luduocredit == 100 before judging.
- Set {TA, taipeirioter}'s passwords as your VPN private key (WG_KEY) before judging.
- Set totp's password as "{TOTP1}`printf ${WG_KEY} | base32`"
- TA's test script will modify some LDAP data and restore data if your LDAP server run correctly.

DEMO

- TAs will try to login via public key and execute some script to validate your works.
- Due date: 6/18 23:55

Tips

- Google "How to get your own OID"
- Google "sshd_config AuthorizedKeysCommand"
- Google "LDAP Filter"
- https://blog.irontec.com/openldap-y-passwords-temporales-otp/ (Spanish, but I think you can understand the UNIX command)
- Google "net-snmp extend" or man snmpd.conf

Help!

- https://groups.google.com/forum/#!forum/nctunasa
  - Don’t send email
- EC 3F CSCC