System Administration HW5

yca

Overview

- Make sure that everything in HW3, HW4 and VPN works.
- Bind NIS server on savpn.nctu.me.
- Mount NFS from savpn.nctu.me.
- Share file with NFS.
- Enable PF and some security settings.

Requirements (1/5)

- NIS Client (15%)
  - Local user still can login to your server.
  - NIS user can login to your server.
  - When an user with an identical name in both NIS and local, then query NIS first.
  - Home directory of NIS user have to be at '/net/home/<username>'.
  - Sharing: hosts, passwd, group, netgroup, ypservers.
  - Test user (password is identical to username.)
    - nisuser1
    - nisuser2
    - nisuser3

Requirements (2/5)

- NFS Client (10%)
  - Mount file from savpn.nctu.me.
    - /net/home
    - /net/data
      - Read only.
  - Do NOT allow set-user-identifier or set-group-identifier bits to take effect.
  - Do NOT allow normal user to mount or unmount.
  - Will be mounted automatically when needed.
    - autofs

Requirements (3/5)

- NFS Server (30%)
  - Exports
    - /net/alpha
    - /net/share
    - /net/admin
  - When someone mount your storage as 'root', they only have permissions same as nobody.
  - Normal user access /net/alpha as their own UID and GID.
  - Normal user access /net/share as UID=user, GID=users.
  - /net/admin is read-only.
  - NFSv4 with `nfsuserd` for mapping UID and username.
  - /etc/exports must be NFSv4 format.

Requirement (4/5)

- Firewall (15%)
  - Deny all connections from <BadHost>.
  - Accept packets from 10.113.0.0/16 to access HTTP/HTTPS.
  - All IP can't send ICMP echo request packets to server. (will NOT response ICMP ECHO-REPLY packets)
    - Except 10.113.0.254.
    - You can add an exception for yourself for testing.
  - Drop packets from <BadGuy> to access FTP and SSH, and response TCP RST/ICMP unreachable.
  - For the table <BadHost> and <BadGuy>, you can test it by yourself or your classmates. *TAs will modify it during DEMO.*

Requirements (5/5)

- If someone attempts to login via SSH but failed for 5 times in 1 hour, then their IP will be banned from SSH for 1 day automatically. (15%)
  - There are many software can do this, e.g. *Blacklistd*, *DenyHosts*, *Fail2Ban*, ...etc. (See appendix.)
  - *TAs will ask you to modify the rules during DEMO.*
  - Banned IP still have access to HTTP/HTTPS.
- Write a shell script 'iamagoodguy' to unban an IP. (5%)
  - Usage: iamagoodguy <IP>
- Your FTP, Web services and VPN work correctly. (10%)

Bonus – Who is the bad guy

- Also apply the rules to FTP. (+5%)
- Log when some IP is banned/unbanned. (+10%)
  - Store at /net/admin/ssh/badguy.log.
  - Format
    - <Time> <IP> is a bad guy, <Count> attempt(s).
    - <Time> <IP> is pardoned by <Sudoer>.
- Use `newsyslog` for log rotation. (+5%)
  - Separated by day, store 10 days.
  - Compressed to '.xz'.

Bonus – Personal webpage for NIS user

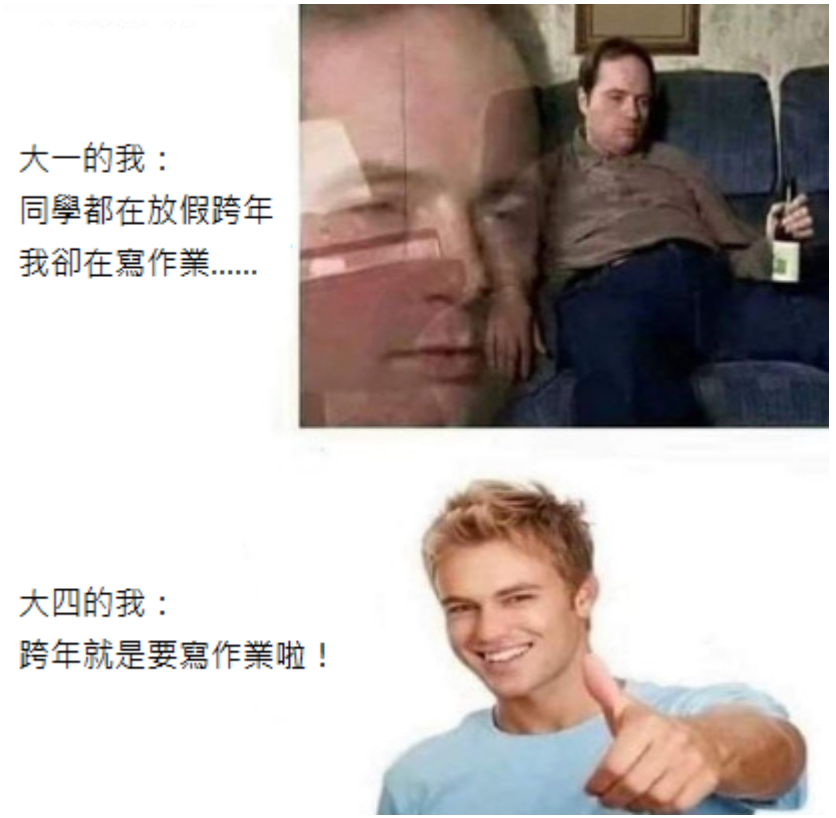
- Personal webpage for NIS user. (+5%)
  - Static webpage in /net/home/{username}/public_html/ with index.html.
  - Accessible on https://{your-domain}/people/~{username}/

Deadline

- 2020/01/08
- You do not need to submit anything.

- Happy New Year!

- 1/11記得去投票！



Help

- E-mail ta@nasa.cs.nctu.edu.tw
- New E3 https://e3new.nctu.edu.tw/
- Office hour: 3GH at CSCC(EC320)

Appendix - Blacklistd

- Blacklistd is a daemon listening to sockets to receive notifications from other daemons about connection attempts that failed or were successful.
- FreeBSD 11 imported blacklistd from NetBSD.
- Enabling Blacklistd
  - The main configuration for blacklistd is stored in blacklistd.conf(5).
  - sysrc blacklistd_enable=yes
  - service blacklistd start

Appendix - DenyHosts

- DenyHosts is a utility developed by Phil Schwartz and maintained by a number of developers which aims to thwart sshd (ssh server) brute force attacks.
- Installation
  - /usr/ports/security/denyhosts
  - pkg install denyhosts
- Enable DenyHosts
  - sysrc denyhosts_enable=yes