Homework 5
NFS & Firewall

cwang, phlin

國立陽明交大資工系資訊中心

Computer Center of Department of Computer Science, NYCU

Outline

- HW 5-1: NFS
  - Server
  - Client
- HW 5-2: Firewall

HW 5-1: NFS (50%)

HW 5-1: Requirements (1/6)

- Set up a NFS server
  - Set up another machine with new IP
    - WireGuard IP: 10.113.254.{ID}
    - WireGuard Private Key: online judge profile
      - WG_NFS_SERVER_PRIVATE_KEY
    - Other settings are the same as HW1
  - Add a user called “judge” for Online Judge on this server
    - All setting is identical to “judge” on your client which you have set on HW1
    - Using "sh" as default shell
    - “judge” needs to run sudo without password
    - Accept “judge” to login your server by our ssh public key

HW 5-1: Requirements (2/6)

- Requirements for NFS server - Export table
    - Restrict other hosts to mount on storage
        - Only 10.113.0.0/24 can mount on /data/public1 and /data/public2
            - Read only
            - export mapping - [HOST]:[EXPORT]
                - /vol/public1 : /net/data/public1
                - /vol/public2 : /net/data/public2
        - Only 10.113.0.{ID}/32 can mount on /data/stu{ID}
            - Allow read & write
            - export mapping - [HOST]:[EXPORT]
                - /vol/stu{ID} : /net/data/stu{ID}
    - When mounting on your storage as “root”, they only have permissions same as “nobody”

HW 5-1: Requirements (3/6)

- Requirements for NFS server - More requirement
  - The minimum NFS server version must be NFSv4
  - /etc/exports must be NFSv4 format
  - Use only reserved port (less than 1024) on NFS
  - Set the port of mountd to 87
- Please make all settings persistent and we will restart your NFS server

HW 5-1: Requirements (4/6)

- Set up a NFS client
  - Some settings are the same as HW1 (Wireguard IP, judge user)
- Requirements for NFS client - Mount and mount automatically
  - Mount three directories on your NFS server (WireGuard IP: 10.113.254.{ID})
    - /net/data/public1, /net/data/public2
      - Read only
    - /net/data/stu{ID}
      - Allow read & write
- Will be mounted automatically when accessed (Hint: autofs)

HW 5-1: Requirements (5/6)

- Requirements for NFS client - More requirement
  - Need to specify to mount with NFSv4
- Requirements for NFS server and client - Check work correctly
  - We will send files to NFS server and NFS client for verification
- Please make all settings persistent and we will restart your NFS client

Grading (50/50%)

- Server
  - Export table (5%)
  - More requirement (5%)
  - Work correctly with client (10%)
- Client
  - Mount successfully (5%)
  - Mount automatically (10%)
  - More requirement (5%)
  - Work correctly with server (10%)

HW 5-2: Firewall (50%)

HW 5-2: Requirements (1/2)

- Accept packet 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.

HW 5-2: Requirements (2/2)

- If someone attempts to login via SSH but failed for 3 times in 1 minute, then their IP will be banned from SSH for 60 seconds automatically.
  - There are many software can do this, e.g. *Blacklistd, DenyHosts, Fail2Ban*, ...etc. (See appendix.)
  - Banned IP still have access to HTTP/HTTPS.

- Write a shell script ‘iamgoodguy’ to unban an IP.
  - Usage : iamgoodguy <IP>

- Your NFS, Web, FTP services and VPN work correctly.

Grading (50/50%)

- All services work correctly (5%)
- HTTP/HTTPS (5%)
- ICMP (5%)
- SSH brute force (30%)
- iamgoodguy script (5%)

Attention!

- Due date: 2021-12-22T23:59:59+08:00
- Online Judge open date: 2021-12-11T23:59:59+08:00

Help me!

- TA time: 3 GH at EC 324 (PC Lab)
- Questions about this homework
  - Ask them on https://groups.google.com/g/nctunasa
  - We MIGHT give out hints on google group
    - Be sure to join the group :D
  - Do not use E3 to email us

Good Luck!

Appendix - Blacklistd

- Blacklistd is a daemon listening to sockets to receive notifications from other daemons about connection attempts that failed or were successful.
- Since 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