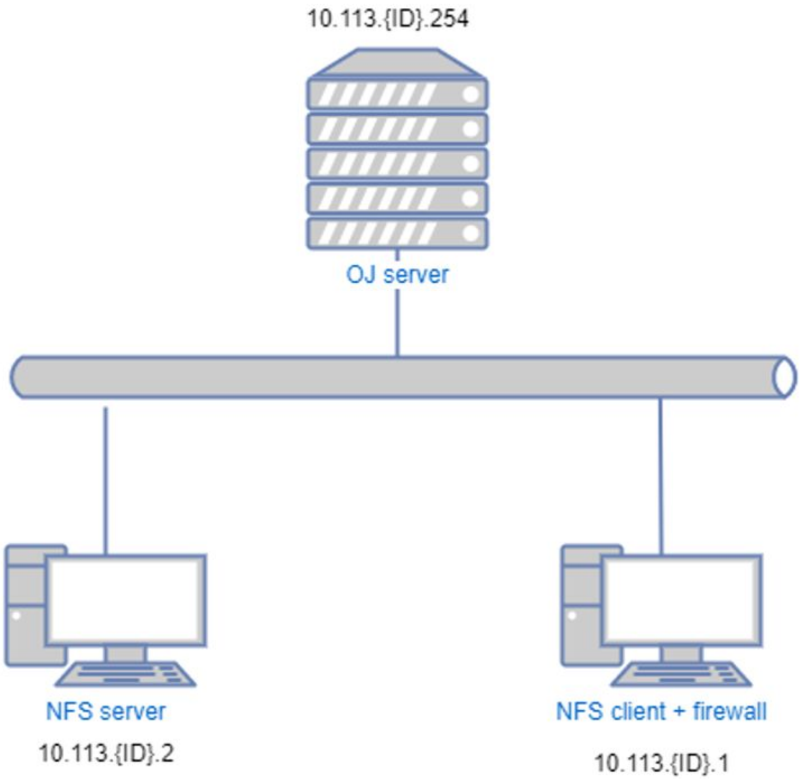
Homework 5
NFS & Firewall

wuph0612, zyyang

Outline & Topology

- HW 5-1: NFS server
- HW 5-2: NFS client
- HW 5-3: Firewall



HW 5-1: NFS server (35%)

HW 5-1: Requirements (1/4)

- Set up NFS server environment
  - Set up another machine with new IP
    - WireGuard IP: 10.113.{ID}.2
    - Example of WireGuard config is on next page
  - Other settings are the same as HW1
    - Add a user called "judge" for Online Judge
    - All setting are identical to “judge” on your client which you have set on HW1
    - User should also be in the "wheel" group
    - Using "sh" as default shell
    - This user needs to run sudo without password

HW 5-1: Requirements (2/4)

- Example of downloaded WireGuard config

```
# [Interface]
# PrivateKey = [WG_PRIVATE_KEY_FOR_INTERFACE1]
# Address = 10.113.$ID.1/32

[Interface]
PrivateKey = [WG_PRIVATE_KEY_FOR_INTERFACE2]
Address = 10.113.$ID.2/32

[Peer]
PublicKey = [WG_SERVER_PUBLIC_KEY]
AllowedIPs = 10.113.0.0/16, 172.16.0.0/16
Endpoint = 140.113.168.131:51011
PersistentKeepalive = 25
```

wg0.conf

HW 5-1: Requirements (3/4)

- Export table
    - Restrict other hosts to mount the storage
        - Only 10.113.{ID}.0/24 can mount /net/data/public
            - Read only
            - export mapping - [HOST]:[EXPORT]
                - /vol/public : /net/data/public
        - Only 10.113.{ID}.1/32 can mount /net/data/stu{ID}
            - Allow read & write
            - export mapping - [HOST]:[EXPORT]
                - /vol/stu{ID} : /net/data/stu{ID}
    - When accessing on your storage as “root”, they only have permissions same as “nobody”

HW 5-1: Requirements (4/4)

- Minimum version

  The minimum NFS server version must be NFSv4

- Exports format

  /etc/exports must be NFSv4 format

- Port number

  Set the port of mountd to 87

- Work correctly with client
  - We will send files to your NFS server for verification

- Others

  Please make all settings persistent and we will restart your NFS server

Grading

- Set up NFS server environment (10%)
- Export table (10%)
- Minimum version (2%)
- Exports format (2%)
- Port number (1%)
- Work correctly with client (10%)

HW 5-2: NFS client (25%)

HW 5-2: Requirements (1/2)

- Mount

  Mount three directories from your NFS server (IP: 10.113.{ID}.1)

  - /net/data/public
    - Read only
  - /net/data/stu{ID}
    - Allow read & write
- Mount automatically

  Will be mounted automatically when accessed (Hint: autofs)

HW 5-2: Requirements (2/2)

- Mounted NFS version
  - Need to specify to mount with NFSv4
- Work correctly with server

Grading

- Mount (6%)
- Mount automatically (6%)
- Mount version (3%)
- Work correctly with server (10%)

HW 5-3: Firewall (40%)

HW 5-3: Requirements (1/2)

- HTTP/HTTPS

  Only accept packet from 10.113.{ID}.0/24 to access HTTP/HTTPS.

- ICMP (ping)

  All IP can’t send ICMP echo request packets to server. (will NOT response ICMP ECHO-REPLY packets)

  - Except 10.113.{ID}.254 and 10.113.{ID}.2
  - You can add an exception of yourself for testing.

HW 5-3: Requirements (2/2)

- SSH failed login

  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.

- iamgoodguy script

  Write a shell script ‘iamgoodguy’ to unban an IP.

  - Usage : iamgoodguy <IP>

Grading

- HTTP/HTTPS (10%)
- ICMP (10%)
- SSH failed login (10%)
- iamgoodguy script (10%)

Attention!

- Your work will be tested by Online Judge system.
  - You can submit multiple judge requests. However, OJ will cool down for several minutes after each judge.
  - **We will take the last submitted score instead of the highest score.**
  - Late submissions will not be accepted.
- BACKUP your server before judge EVERY TIME
  - We may do something bad when judging.
- Make sure everything is fine after reboot.

```
# rm -rf /*
```

Attention!

- TAs reserve the right of final explanations. Specs and the points of each sub-judges are subject to change in any time.
- **Start from 2022/12/22 21:00**
- **Deadline 2023/01/11 23:59**

Help me!

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
  - When posting a question, be sure to include all information you think others would need
    - including but not limiting to your ID, setups, configurations and / or what you have done to trace the error / problem
- Do not email us
- 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