

Homework 4

Web Services & Firewall

prlin, enchen

國立陽明交通大學資工系資訊中心

Information Technology Center of Department of Computer Science, NYCU

Outline

- HTTP Server (65%)
 - Virtual Hosts (6%)
 - Logging (6%)
 - Log Rotate (6%)
 - HTTPS & HTTP2 (15%)
 - Hide Server Information (5%)
 - Access Control (6%)
 - PHP / PHP-FPM (6%)
 - HTTP3 (15%)
- Firewall (35%)
 - ICMP (5%)
 - Web Services (10%)
 - SSH/Web failed login (10%)
 - iamgoodguy script (10%)

HTTP Server

Reminders

- No matter which OS, use **10.113.{ID}.11** to do this homework
- You will be asked to prepare a web server with HTTP/3 enabled.
 - However, currently most common web servers, like Nginx/Apache, **do not come with built-in HTTP/3**.
- Some recommended ways are
 - Build a web server with HTTP/3 on your own **in advance**
 - Install another web servers with built-in HTTP/3, like Caddy
- For detailed spec, please refer to problem **HTTP/3** on p.17

Virtual Host (6%)

- Setup a name-based virtual host.
- Show different contents based on different domain / IP.
 - Your Domain Name: {ID}.cs.nycu
 - Your IP: 10.113.{ID}.11
 - {ID} is your wireguard ID

Hint:

You can use hosts file to map ip to your domain.

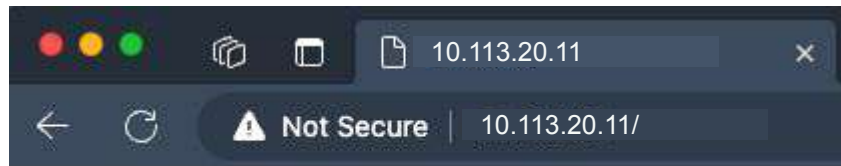
- On FreeBSD, CentOS, Ubuntu: */etc/hosts*
- On Windows: *C:\Windows\System32\drivers\etc\hosts*

Virtual Host (6%)

- Requirements for contents in different domain are:
 - Domain: http://{ID}.cs.nycu
 - Content: 2023-nycu.sa-hw4-vhost
 - File path: /home/judge/www/{ID}.cs.nycu/index.html
 - IP: http://10.113.{ID}.11
 - Content: 2023-nycu.sa-hw4-ip
 - File path: /home/judge/www/10.113.{ID}.11/index.html



2023-nycu.sa-hw4-vhost



2023-nycu.sa-hw4-ip

Logging (6%)

- Set the following logging format on 10.113.{ID}.11
- Log Format
 - Combined: default in Nginx, or custom log format with the **circled** part
 - Agent: “\$remote_addr | \$request | \$http_user_agent is my Agent Info.”

```
1 // access.log
2 127.0.0.1 - - [01/Nov/2023:03:40:05 +0000] "GET / HTTP/1.1" 200 20 "-" "curl/7.81.0"
3
4 // compressed.log.gz
5 127.0.0.1 | GET / HTTP/1.1 | curl/7.81.0 is my Agent Info.
6
```

Logging (6%)

- Write access logs to
 - **/home/judge/log/access.log**
 - Log Format: Combined
 - **/home/judge/log/compressed.log.gz**
 - Log Format: Agent
 - Compressed in **gzip** format, flush in **5** seconds
- **We will test your logging setting by sending some requests first**

Log Rotate (6%)


- Log rotate your web server's log files
 - logrotate [[Ubuntu](#), [FreeBSD](#)]
 - Logrotate target: **/home/judge/log/access.log**
- Requirements
 - Logrotate if file size is greater than 150 bytes
 - If less than 150 bytes, do nothing
 - Reserve only 3 rotate files
 - Compress with gzip
- Save your config in **/home/judge/log/judge-rotate.conf**

HTTPS & HTTP/2 (15%)

- On virtual host **{ID}.cs.nycu**
 - Enable HTTPS with certificate from our CA server (5%)
 - CA Server: <https://ca.nasa.nycu:9000/acme/acme/directory>
 - Map ip 10.113.200.1 to domain ca.nasa.nycu
 - **Trust** [Root CA](#) for CA server to work
 - Default certificate expires in **one** month

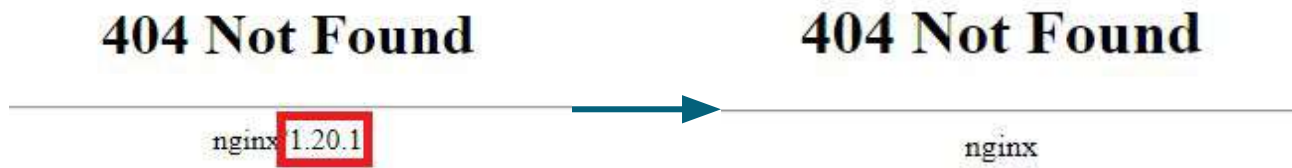
HTTPS & HTTP/2 (15%)

- On virtual host `{ID}.cs.nycu`
 - Redirect all HTTP requests to HTTPS. (3%)
 - Enable HSTS (HTTP Strict Transport Security) (2%)
 - Enable HTTP/2 with HTTPS (5%)

Name	Status	Proto...	Type	Initiator
 20.cs.nycu	301	http/1.1	doc...	Other
 20.cs.nycu	200	h2	doc...	20.cs.nycu/

Hide Server Information (5%)

- On virtual host `{ID}.cs.nycu`
 - Do not show the server version on error pages.



- Hide Nginx/Apache version in header.

```
▼ Response Headers
accept-ranges: bytes
content-length: 18
content-type: text/html
date: Tue, 23 Nov 2021 06:29:56 GMT
etag: "619bc315-12"
last-modified: Mon, 22 Nov 2021 16:19:33 GMT
server: nginx/1.20.1
strict-transport-security: max-age=31536000; includeSubDomains
```

```
▼ Response Headers
accept-ranges: bytes
content-length: 18
content-type: text/html
date: Tue, 23 Nov 2021 07:24:38 GMT
etag: "619bc315-12"
last-modified: Mon, 22 Nov 2021 16:19:33 GMT
server: nginx
strict-transport-security: max-age=31536000; includeSubDomains
```

Access Control (6%)

- On virtual host 10.113.{ID}.11
 - There is a secret webpage on http://10.113.{ID}.11/private
 - Content: nycu-sa-hw4-private
 - Deny access with domain {ID}.cs.nycu
 - Only allow access from 10.113.{ID}.254 and 127.0.0.1
 - Request with domain or not from specified IP
 - Return 403 Forbidden or 404 Not Found

Access Control (6%)

- On virtual host 10.113.{ID}.11
 - When accessed from localhost, the user is required to provide credentials (HTTP Basic Authentication).
 - Username: sa-admin
 - Password: Your {IP} without dots. (e.g. 101132011)



登錄以存取此網站

http://10.4.2.242 要求授權
此網站的連線不安全

使用者名稱:

密碼:



PHP / PHP-FPM (6%)

- On virtual host **{ID}.cs.nycu**
 - Create <https://{ID}.cs.nycu/info-{ID}.php> with PHP info page.
 - Set up PHP 8.2 (or higher).
 - Hide PHP version information in header.
 - But the version needs to be displayed in the PHP info page.

PHP / PHP-FPM (6%)

PHP Version 8.2.11

php version >= 8.2



System	FreeBSD 2023-ss-hw4-freebsd-test 13.2-RELEASE FreeBSD 13.2-RELEASE releng/13.2-n254617-525ecfdd597 GENERIC amd64
Build Date	Nov 9 2023 01:29:36
Build System	FreeBSD 132amd64-quarterly-jcb-07 13.2-RELEASE-p5 FreeBSD 13.2-RELEASE-p5 amd64
Configure Command	'./configure' '--disable-all' '--program-prefix=' '--with-config-file-scan-dir=/usr/local/etc/php' '--with-layout=GNU' '--with-libxml' '--with-openssl' '--with-password-argon2=/usr/local' '--enable-dtrace' '--enable-embed' '--enable-fpm' '--with-fpm-group=www' '--with-fpm-user=www' '--enable-mysqlnd' '--prefix=/usr/local' '--localstatedir=/var' '--mandir=/usr/local/man' '--infodir=/usr/local/share/info' '--build=amd64-portsbsd-freebsd13.2' 'build_alias=amd64-portsbsd-freebsd13.2' 'PKG_CONFIG=pkgconf' 'PKG_CONFIG_LIBDIR=/workdirs/usr/ports/lang/php62/work/pkgconfig /usr/local/libdata/pkgconfig /usr/local/share/pkgconfig /usr/libdata/pkgconfig' 'CFLAGS=-O2 -pipe -fstack-protector-strong -fno-strict-aliasing' 'LDFLAGS=-L/usr/lib -lcrypto -lssl -fstack-protector-strong' 'CXXFLAGS=-O2 -pipe -fstack-protector-strong -fno-strict-aliasing' 'OPENSSL_CFLAGS=-I/usr/include' 'OPENSSL_LIBS=-L/usr/lib -lssl -lcrypto'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc
Loaded Configuration File	/usr/local/etc/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php
Additional .ini files parsed	(none)
PHP API	20220829
PHP Extension	20220829
Zend Extension	420220829
Zend Extension Build	API420220829,NTS
PHP Extension Build	API20220829,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
Zend Max Execution Timers	disabled
IPv6 Support	enabled
DTrace Support	available, disabled

Network

Filter: ☐ Preserve log ☒ Disable cache No throttling ☐ Hide data URLs ☐ Hide extension URLs

All Doc JS Fetch/XHR CSS Font Img Media Manifest WS Wasm Other

☐ Blocked response cookies ☐ Blocked requests ☐ 3rd-party requests

500 ms 1000 ms 1500 ms 2000 ms 2500 ms 3000 ms 3500 ms 4000 ms 4500 ms

Name X Headers Preview Response Initiator Timing

in... d... d...

General

Request URL: https://20.cs.nyu.edu/info-20.php

Request Method: GET

Status Code: 200 OK

Remote Address: 10.4.2.98:443

Referer Policy: strict-origin-when-cross-origin

Response Headers

Content-Type: text/html; charset=UTF-8

Date: Thu, 23 Nov 2023 15:10:13 GMT

Server: nginx

Strict-Transport-Security: max-age=31536000; includeSubDomains

Request Headers

no php version in header

authority: 20.cs.nyu.edu

method: GET

path: /info-20.php

scheme: https

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp/e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-TW,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Cache-Control: no-cache

Pragma: no-cache

Sec-Ch-Ua: "Microsoft Edge";v="119", "Chromium";v="119", "Not?A_Brand";v="

HTTP/3 (15%)

- Set up a web server with HTTP/3 support on port 3443
- Build a [curl](#) from source code with HTTP/3 support
 - Make it available as *curl_http3* from any location
 - [Curl with HTTP3 and QUIC](#)
- Build a web server with HTTP/3 or Install web server with HTTP/3
 - Reference: [Nginx](#) with HTTP/3, [Caddy](#)

```
root@enchen-SA:~/curl_http3/curl/src# curl_http3 --version
curl 8.5.0-DEV (x86_64-pc-linux-gnu) libcurl/8.5.0-DEV quictls/3.1.4 nghttp2/1.43
.0 ngtcp2/1.0.1 nghttp3/1.0.0
Release-Date: [unreleased]
Protocols: dict file ftp ftps gopher gophers http https imap imaps mqtt pop3 pop3
s rtsp smb smbs smtp smtps telnet tftp
Features: alt-svc AsynchDNS HSTS HTTP2 HTTP3 HTTPS-proxy IPv6 Largefile NTLM SSL
threadsafe TLS-SRP UnixSockets
```

```
> HTTP/3 200
< server: Caddy
< content-type: text/plain; charset=utf-8
< date: Wed, 22 Nov 2023 17:28:19 GMT
< content-length: 21
<
```

HTTP/3 (15%)

- Enable HTTP/3 with self-signed certificate
 - Please sign your own certificate on your domain using openssl.
 - Self-signed certificate subject information:
 - CN={ID}.cs.nycu, OU=2023SA, O=NYCU, L=Hsinchu, ST=Hsinchu, C=TW
- You can test HTTP/3 server with browser or curl_http3
- **Make HTTP/3 work on localhost is enough**
 - Since remote request to HTTP/3 servers on port 3443 would be downgraded by browsers

Firewall

Firewall: Requirements (1/2)

- 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
- You can add an exception of yourself for testing.

- Web Services

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

- HTTP/HTTPS (tcp)
- HTTP/3 (tcp, udp)

Firewall: Requirements (2/2)

- SSH/Web Service failed login

If someone attempts to login via SSH/Web but failed for 3 times in 5 minute, then their IP will be banned from SSH/Web for 60 seconds automatically.

- There are many software can do this, e.g. Blacklisted, DenyHosts, Fail2Ban, ...etc. (See appendix.)
- Banned SSH still have access to other services.
- Banned HTTP/HTTPS still have access to other services.

- iamgoodguy script

Write a shell script 'iamgoodguy' to unban an IP.

- Usage: iamgoodguy <IP> -p <ssh|web>
- Ensure the **judge** user operates without permission restrictions.

Hints

1. You can use **any webserver** to complete this homework, but only Nginx is guaranteed to pass.
2. If you find your system too slow, please consider adding more RAM to it.
3. Please configure the firewall with the strictest settings.
 - > FreeBSD:block all
 - > Ubuntu:INPUT Chain DROP

Homework 4

1. BACKUP your server before judge EVERY TIME.
2. We may do some things bad when judging.
3. TAs reserve the right of final explanations. Specs and the points of each sub-judges are subject to change in any time.
4. We might randomly pick some student to demo after the end of HW4.
5. Start: 2023/12/01 00:00
6. Deadline: 2023/12/22 23:59

Help me! TA!

- 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 use E3 to email us.

Good Luck!

國立陽明交通大學資工系資訊中心

Information Technology Center of Department of Computer Science, NYCU

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/denylhosts`
 - `pkg install denyhosts`
- Enable DenyHosts
 - `sysrc denyhosts_enable=yes`