(/)

Curriculum

SE Foundations

Average: **108.76%**

0x13. Firewall

DevOps **SysAdmin** **Security**

By: Sylvain Kalache, co-founder at Holberton School

Weight: 1

Project over - took place from Sep 18, 2023 6:00 AM to Sep 19, 2023 6:00 AM

☑ An auto review will be launched at the deadline

In a nutshell…

- **Auto QA review:** 7.0/7 mandatory & 2.0/2 optional
- **Altogether: 200.0%**
  - Mandatory: 100.0%
  - Optional: 100.0%
  - Calculation: 100.0% + (100.0% * 100.0%) == **200.0%**

Concepts

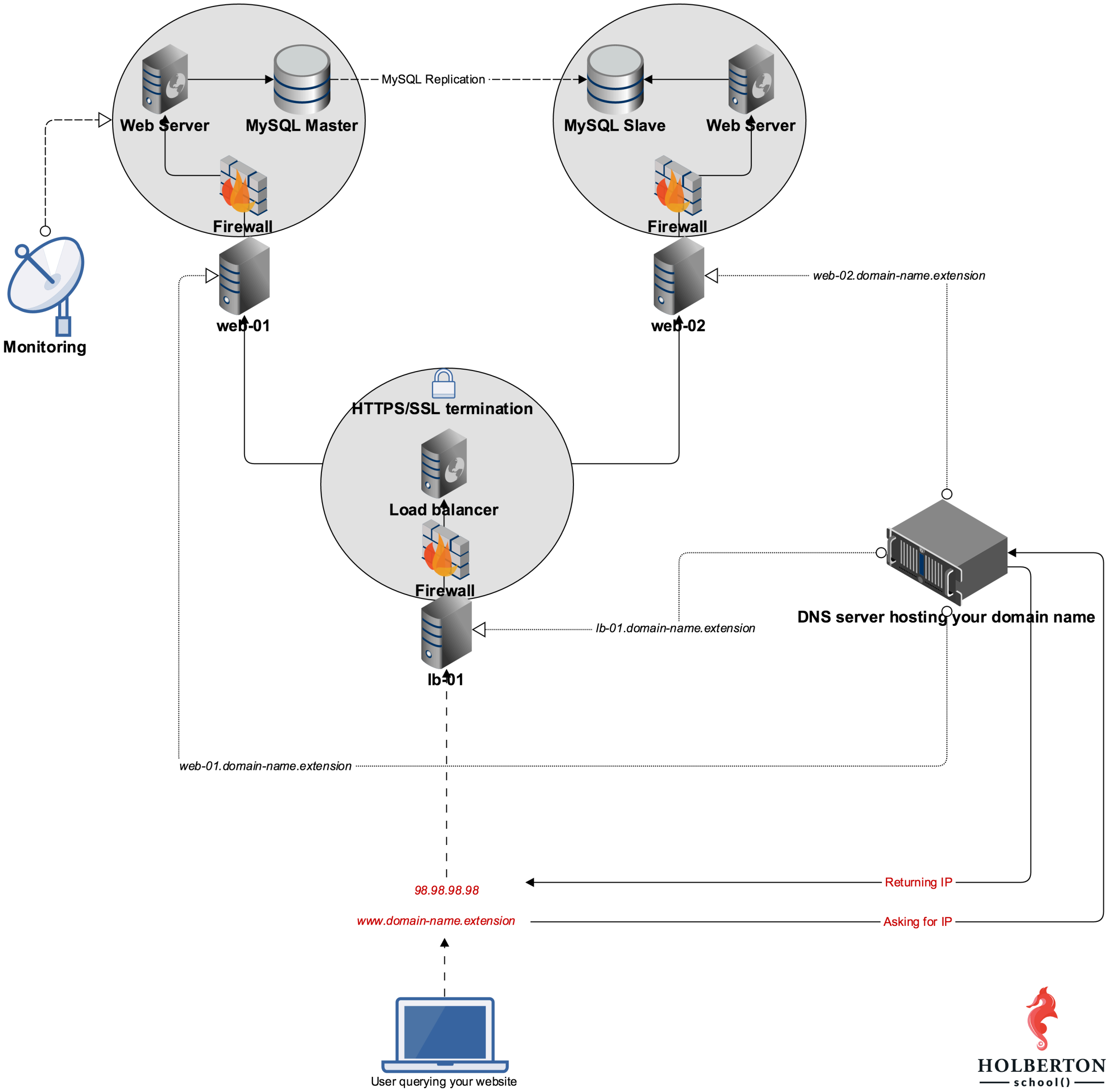
For this project, we expect you to look at this concept:

- Web stack debugging (/concepts/68)

Help

(/)

Firewall


MySQL Replication
Web Server
MySQL Master
MySQL Slave
Web Server
Firewall
Firewall
Monitoring
web-01
web-02
web-02.domain-name.extension
HTTPS/SSL termination
Load balancer
Firewall
lb-01
lb-01.domain-name.extension
DNS server hosting your domain name
web-01.domain-name.extension
98.98.98.98
Returning IP
www.domain-name.extension
Asking for IP
User querying your website

Background Context

Your servers without a firewall…

Resources

Read or watch:

- What is a firewall (/rltoken/vjB4LyHRdtEImzZcuD89ZQ)

More Info

As explained in the **web stack debugging guide** concept page, `telnet` is a very good tool to check if sockets are open with `telnet IP PORT`. For example, if you want to check if port 22 is open on `web-02`:

```
sylvain@ubuntu$ telnet web-02.holberton.online 22
Trying 54.89.38.100...
Connected to web-02.holberton.online.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8

Protocol mismatch.
Connection closed by foreign host.
sylvain@ubuntu$
```

We can see for this example that the connection is successful: `Connected to web-02.holberton.online.`

Now let's try connecting to port 2222:

```
sylvain@ubuntu$ telnet web-02.holberton.online 2222
Trying 54.89.38.100...
^C
sylvain@ubuntu$
```

Score: 100.0% (*Checks completed: 100.0%*)

(/)

Let’s install the `ufw` firewall and setup a few rules on `web-01`.

Requirements:

- The requirements below must be applied to `web-01` (feel free to do it on `lb-01` and `web-02`, but it won’t be checked)
- Configure `ufw` so that it blocks all incoming traffic, except the following TCP ports:
  - `22` (SSH)
  - `443` (HTTPS SSL)
  - `80` (HTTP)
- Share the `ufw` commands that you used in your answer file

Repo:

- GitHub repository: `alx-system_engineering-devops`
- Directory: `0x13-firewall`
- File: `0-block_all_incoming_traffic_but`

☑ Done! | Help | Check your code | >_ Get a sandbox | QA Review

1. Port forwarding

#advanced

Score: 100.0% (*Checks completed: 100.0%*)

Firewalls can not only filter requests, they can also forward them.

Requirements:

- Configure `web-01` so that its firewall redirects port `8080/TCP` to port `80/TCP`.
- Your answer file should be a copy of the `ufw` configuration file that you modified to make this happen

Terminal in `web-01`:

```
root@03-web-01:~# netstat -lpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/
Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      247
3/nginx
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      978/
sshd
tcp6       0      0 :::80                   :::*                    LISTEN      247
3/nginx
tcp6       0      0 :::22                   :::*                    LISTEN      978/
sshd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           594/
dhclient
udp        0      0 0.0.0.0:54432           0.0.0.0:*                           594/
dhclient
udp6       0      0 :::32563                :::*                                594/
dhclient
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name    Path
unix  2      [ ACC ]     SEQPACKET  LISTENING     7175     433/systemd-udevd   /run/
udev/control
unix  2      [ ACC ]     STREAM     LISTENING     6505     1/init              @/co
m/ubuntu/upstart
unix  2      [ ACC ]     STREAM     LISTENING     8048     741/dbus-daemon     /var/
run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     8419     987/acpid           /var/
run/acpid.socket
root@03-web-01:~#
root@03-web-01:~# grep listen /etc/nginx/sites-enabled/default
    listen 80 default_server;
    listen [::]:80 default_server ipv6only=on;
    # pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000
#   listen 8000;
#   listen somename:8080;
#   listen 443;
root@03-web-01:~#
```

- My web server `nginx` is only listening on port `80`
- `netstat` shows that nothing is listening on `8080`

Terminal in `web-02`:

```
ubuntu@03-web-02:~$ curl -sI web-01.holberton.online:80
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 07 Mar 2017 02:14:41 GMT
Content-Type: text/html
Content-Length: 612
Last-Modified: Tue, 04 Mar 2014 11:46:45 GMT
Connection: keep-alive
ETag: "5315bd25-264"
Accept-Ranges: bytes

ubuntu@03-web-02:~$ curl -sI web-01.holberton.online:8080
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 07 Mar 2017 02:14:43 GMT
Content-Type: text/html
Content-Length: 612
Last-Modified: Tue, 04 Mar 2014 11:46:45 GMT
Connection: keep-alive
ETag: "5315bd25-264"
Accept-Ranges: bytes

ubuntu@03-web-02:~$
```

I use curl to query `web-01.holberton.online` , and since my firewall is forwarding the ports, I get a `HTTP 200` response on port `80/TCP` and also on port `8080/TCP` .

Repo:

- GitHub repository: `alx-system_engineering-devops`
- Directory: `0x13-firewall`
- File: `100-port_forwarding`

☑ Done! Help Check your code >_ Get a sandbox QA Review