UC Berkeley CS 168, Fall 2014

CS168 Project 3b

(Version 1.0)

Due: 11:59:59am (at noon), December 3rd, 2014 (Hard deadline)

Anurag Khandelwal Shoumik Palkar Sangjin Han

Overview

In this project, you will implement a basic firewall running at end hosts. A firewall is a "*security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on a rule set*" [Wikipedia]. Unlike the previous projects of this course, where you worked in simulated environments, you will deal with real packets in a Linux-based virtual machine (VM) for this project.

Recall that in 3a, you implemented a stateless passive firewall: that is, your firewall could do its job by considering each packet individually, and it did not generate traffic.

In 3b, you will be extending your solution for 3a to make a stateful active application-layer firewall. You will use the same framework, VM, test harnesses, tools, and as in 3a. Now, your firewall should generate packets in response to denied packets. Upon completing this part, you should:

- Be familiar with the HTTP and DNS protocols.
- Understand the difference between stateful vs. stateless, active vs. passive firewalls.

Besides writing code, you will need to (and should) spend a lot of time to understand protocol specifications, to design algorithms, and to test your application. Start working on the project as soon as possible.

You will likely find the supplementary document from 3a useful for this part, as well.
http://www-inst.eecs.berkeley.edu/~cs168/fa14/projects/project3a/supplement.pdf

Good luck, and have fun.

Changelog

Always check the latest version of this document. It is your responsibility that your solution conforms to the latest version of the spec.

v1.0 (11/17/2014)

- First release

Requirements

Overview

In the project, you must implement three new rules (The rules filename will be still given with `config['rule']` as in 3a).

1. `deny tcp <IP address> <port>`
2. `deny dns <domain name>`
3. `log http <host name>`

The format of `IP address`, `port`, and `domain name` are defined in the same way as in Project 3a. For `host name`, see below.

Firewall behavior from Project 3a will remain the same, for instance you should still "pass a packet if none matches" and "follow the verdict of the last matching rule". **However, for Project 3b, we will neither test firewall rules defined in 3a (`pass`/`drop` rules) nor country-based matching,** so your grade for 3a will be mostly decoupled from your grade for 3b. If your solution for 3a was incomplete, don't worry too much.

For the sake of simplicity, you can make the following assumptions:

- The rules file has always correct syntax, as defined in Project 3a.
- All packets seen by the firewall are neither corrupted nor malformed.
- All TCP connections with external port 80 are valid HTTP connections.
    - However, your HTTP header parser should not be overly restrictive. Many web servers in the wild have slightly different implementations, and your parser should be flexible enough to parse them correctly. For example, `content-length` (not `Content-Length`) is a valid header field name. When in doubt, consult RFC 2616.
    - Also, you should be able to deal with out-of-order TCP packets, caused by reordering, drop, or loss. See below for details.

1. Injecting RST Packets: `deny tcp`

In addition to dropping a matching TCP packet, respond to the initiator `(src addr, src port)` with a TCP packet with the RST flag set to 1.

If you simply drop these packets (with a `drop` rule), then the client application will try sending SYN packets several times over the course of a minute or so before giving up. However, if you also send a RST packet to the client (with a `deny` rule), the application will give up immediately.

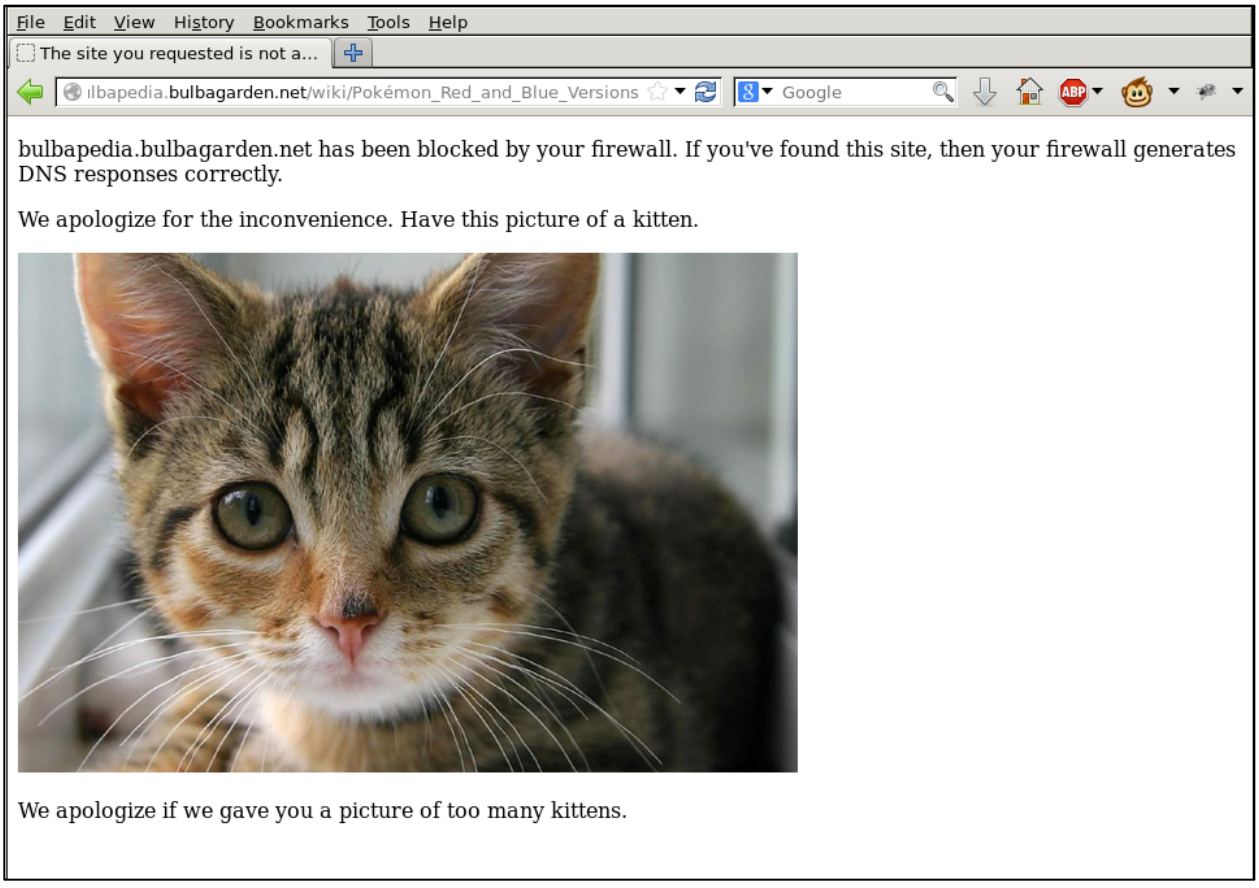
When generating the reset packet you must carefully compute both the TCP and IPv4 checksum; consult Wikipedia or the relevant RFCs for details. http://locklessinc.com/articles/tcp_checksum/ also has some C code (go through the `checksum1()` function) that might help you figure out how to implement these. Please do not copy checksum code directly from the Internet, as we will be using tools to detect copied code.

2. Injecting DNS Response Packets: `deny dns`

In addition to dropping a matching DNS request, send a DNS response to the internal interface pointing to the fixed IP address `54.173.224.150`. Consult section 4.1.1 and 4.1.3 of RFC 1035.

If the QTYPE of a matched DNS request is **AAAA**, drop the packet, and do not send a response.

If you implement this correctly, then your browser will direct you to a placeholder website. Your response should be in the **answer section** should have type **A** (i.e. it is an address) and a TTL of 1 second. Make sure you copy the ID field as appropriate and the RCODE field as appropriate.



If your firewall generates DNS rules properly, you should see a page similar to this.

3. HTTP Log: `log http`

For matching host names, log HTTP transactions over TCP connections with external port 80 to `http.log` in the current directory. An HTTP transaction is defined as a **pair of an HTTP request and an HTTP response**. For each transaction, leave a log according to the following format (space-delimited) in a single line:

```
host_name method path version status_code object_size
```

To understand what these values log, consider the following HTTP request:

```
GET / HTTP/1.1
Host: google.com
User-Agent: Web-sniffer/1.0.46 (+http://web-sniffer.net/
Accept-Encoding: gzip
Accept-Charset: ISO-8859-1,UTF-8;q=0.7,*;q=0.7
Cache-Control: no-cache
Accept-Language: de,en;q=0.7,en-us;q=0.3
```

And the corresponding response:

```
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Date: Mon, 18 Nov 2013 23:58:12 GMT
Expires: Wed, 18 Dec 2013 23:58:12 GMT
Cache-Control: public, max-age=2      592000
Server: gws
Content-Length: 219
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Alternate-Protocol: 80:quic
```

For this example you would log the following (word in this section means words as in parts of a sentence, i.e., whitespace separated values):

- `host_name`: Use the value of `Host` request header field. If it is not present, use the external IP address of the TCP connection. (In the above `host_name` is google.com)
- `method`: The first word of the request line (e.g. `GET`, `POST`, `PUT`, `DROP`). It will be mostly `GET`.
- `path`: The second word of the request line. (`/` in this case)
- `version`: The third word of the request line (e.g., `HTTP/1.0` or `HTTP/1.1`) (in this case HTTP/1.1)
- `status_code`: The second word of the response line. (in this case `301`)
- `object_size`: Use the `Content-Length` response header field. Its value will be identical to the actual HTTP response payload size. If this field is not present, then this field should be -1. (In this case it is 219).

Hostname Matching

`host name` in an http rule can be either a domain name or a single IPv4 address (neither prefix nor `any`). Domain names (full/wildcard) are used in the same way as in Project 3a. The following shows some examples of valid hostnames.

- `google.com`
  - only matches google.com
- `*.facebook.com`
  - matches foo.facebook.com and bar.baz.facebook.com, but not facebook.com
- 123.45.67.89
  - matches 1) if the Host header field value is 123.45.67.89, or
    2) if the Host header field is not present and the external IP address is 123.45.67.89.
- *
  - matches every HTTP request.

Those host names are matched against the `Host` header field value in HTTP requests. If the header is not present, use the external IP address in the quad-dotted notation as a fallback.

If multiple http rules match, log the transaction only once.

Notes and Hints

Packets to inspect:

- Note that since we assume you are not running a web server on port 80, the external port for requests should be the destination port, and the external port for responses should be the source port.
- You can assume that all TCP traffic on port 80 is actually HTTP.
- Because we only check port 80 for HTTP, this cannot match HTTPS (nor should it), whose default port number is 443.

Log file:

- The name of log file is fixed: `http.log` (in the current directory)
- Your firewall should append to an existing log file, or create it if it does not exist.
  - `f = open('http.log', 'a')` will do this for you.
- **Flush the log file after each write, with `f.flush()`**
  - If you don't call `f.flush()` after each write, the your firewall process would keep buffering data and delay actual writes to the file for unpredictable amounts of time.
  - This could mean the autograder sees nothing written by your firewall during grading.
  - In short, `f.flush()` after each use!

TCP reassembly

- The communication between HTTP applications (web browser/server) with a byte stream for each direction. What your firewall sees is packets segmented by the TCP layer. To parse HTTP requests and responses, you should reassemble TCP segments into byte streams, based on the TCP sequence numbers. This process is similar to what the "Follow TCP Stream"

feature does in Wireshark (see the supplementary document).

- The HTTP request/response header may span multiple packets.
  - One common example: an HTTP request/response header is bigger than MSS, so it is broken into multiple TCP packets.
  - One extreme example: suppose an HTTP request is segmented into single-byte TCP packets, i.e., “G”, “E”, “T”, “ ”, “/”, “ ”, “H”, “T”, “T”, “P”, … Can your firewall handle this case?
- Packets may be dropped/reordered arbitrarily. To make it easier to handle this we suggest you drop *out-of-order packets with a forward gap*, on a per-connection basis, for each direction, so that both the endpoint and the firewall only process in-order packets. TCP RTO will ensure that packets are retransmitted. While this negatively impacts performance, it simplifies code and reduces the amount of state that your firewall needs to maintain.
  - Suppose you were expecting SEQ 4000 for the next packet. If you get a TCP packet with SEQ 5000, you drop the packet.
  - On the other hand, if you get a TCP packet with SEQ 3000, you should **pass** the packet, since it indicates retransmission of lost packets. If you drop the packet, the connection will be stuck.
- Note that TCP sequence numbers are 32-bit unsigned integers, so they can *wrap around*.
- Assume that HTTP is not pipelined (we disabled this feature in Firefox), so requests and responses always begin at the beginning of the payload of a TCP packet.

Dealing with Persistent HTTP Connections

- You should handle persistent HTTP connections. If a connection is persistent (refer to http://en.wikipedia.org/wiki/HTTP_persistent_connection), then message length will be specified via `Content-Length` (which we define as the HTTP payload size in bytes, excluding the header).
- Responses to `HEAD` request do not have HTTP payload, but they may have non-zero `Content-Length` values (section 14.13 in the RFC document).
- Note that HTTP requests may have non-empty payload (e.g., `POST` method)

Others

- Your firewall must support concurrent HTTP connections. It is typical that a web browser opens tens of connections to access a web page.
  - Also, dropping out-of-order packets should be done on a per-connection basis.
- Your implementation must not waste memory unnecessarily. For example, when you download a large file via HTTP, your firewall should not store the entire byte stream. You only need to buffer partial HTTP headers.
- Again, your firewall should not crash.

Examples

1. Consider "`log http *.berkeley.edu`". Opening http://www-inst.eecs.berkeley.edu/~cs168/fa14 in Firefox will produce the following log entries, after clearing the browser cache:

```
www-inst.eecs.berkeley.edu GET /~cs168/fa14 HTTP/1.1 301 254
www-inst.eecs.berkeley.edu GET /~cs168/fa14/ HTTP/1.1 200 273
www-inst.eecs.berkeley.edu GET /~cs168/fa14/overview.html HTTP/1.1 200 2581
www-inst.eecs.berkeley.edu GET /~cs168/fa14/content.html HTTP/1.1 200 1569
www.eecs.berkeley.edu GET /Includes/EECS-images/eecslogo.gif HTTP/1.1 200 828
www-inst.eecs.berkeley.edu GET /~cs168/fa14/images/Keycard_A.png HTTP/1.1 200 324
www-inst.eecs.berkeley.edu GET /~cs168/fa14/images/Book.png HTTP/1.1 200 174
www-inst.eecs.berkeley.edu GET /favicon.ico HTTP/1.1 200 0
```

Details (the ordering, fetched objects, or their size) may vary, due to various reasons.

2. Consider "`log http *`". In a terminal window, "`wget google.com`" will produce the following log entries (again, details may vary).

```
google.com GET / HTTP/1.1 301 219
www.google.com GET / HTTP/1.1 200 -1
```

Note that in Example 1, the request for favicon.ico explicitly specified `Content-Length` as 0, whereas in Example 2, the request to `www.google.com` for `/` did not specify a `Content-Length`, so we used the placeholder value of -1.

Logistics

Collaboration Policy

The project is designed to be solved independently, but you may work with your partner from 3a, if you wish. **You may not work with someone new, unless both you and your new partner worked alone for 3a.** Grading will remain the same whether you choose to work alone or in partners; both partners will receive the same grade regardless of the distribution of work between the two partners.

By the nature of this project, it could be hard to "split" the work between teammates. Instead, consider pair programming (http://en.wikipedia.org/wiki/Pair_programming), if you choose to work in partners.

Submission Instructions

Turn in a `.tar` file with both you and your partner's last names in the file name (For example, `project3b-khandelwal-palkar.tar` or `project3b-han.tar`) on an instructional machine. Your tar file should include:

- `firewall.py`: remember, this file should include all your code.
- `readme.txt`
  - Your (and your partner's) full name and login name.
  - (optional) Any comments/concerns on the project. This will not affect grading. We will collect your opinions anonymously to design future projects better.

```
$ tar --cf project3b-han.tar firewall.py readme.txt
$ submit project3b
```

Note: **We always use the latest submission.**

Regrade & Late Policy

Your regrade request must be made within seven days after score release. Submit your new tar file on an instructional machine, then email anuragk@eecs.berkeley.edu.

- final score = max{old score, new score * (regrading penalty)} * (your original late penalty)
  - regrading penalty = 0.9 - (code difference in bytes) * 0.001
    - We will provide a script that measures code difference.
  - Of course, regrading penalty doesn't apply if it turns out be auto-grader's fault.
- You have only one opportunity for regrade request.

The late policy is simple; no slip dates. If submission is late, it is penalized as follows:

- < 24 hours late, you lose 10%
- < 48 hours, 20%
- < 72 hours, 40%
- More than three days late, you can no longer hand-in the assignment.

Cheating

Simply put, DO NOT EVER TRY IT. We will do our best to protect our students from losing the value of their honestly earned grades due to cheaters. We may perform manual inspection and use automated tools (do not underestimate them) to detect potential plagiarism over all submissions.

Refer to the course webpage for more information. If you are not sure what may constitute cheating, consult the instructor or GSIs. Assignments suspected of cheating or forgery will be handled according to the Student Code of Conduct[1]. Apparently 23% of academic misconduct cases at a certain junior university are in Computer Science[2], but we expect you all to uphold high academic integrity and pride in doing your own work.

[1] http://sa.berkeley.edu/code-of-conduct
[2] http://www.pcworld.com/article/194486/Computer_Science_Students_Cheating.html

DO's and DON'Ts

DO's

- It is okay to use external libraries or applications to **test** your firewall.
- You can modify not only `firewall.py` but also other source code files, but only for debugging purposes.
    - Do remember that you only submit the `firewall.py` file, and it should work with the original code of other files.
- Backup is always a good idea.
- Feel free to surf the Web for **general ideas**, such as Python language/library references, network protocol specifications, testing tool usages, and debugging tips.
    - Admittedly, Google is faster and more accurate than GSIs in most cases. Also it works 24/7.
- You can discuss with anyone algorithms, approaches, and concepts without details, but stay away from your computer/code while doing so.
- We encourage you to share test strategies with your fellow students on Piazza, but only at the high level (e.g., no test code).
- We recommend using Firefox in the VM, rather than installing other web browsers. The Firefox installed in the VM was specially configured to suppress some seemingly strange behaviors.

DON'Ts

- Do not create extra threads or processes.
- Do not use any libraries other than Python 2.7 standard modules to implement the firewall.
- Do not alter the network configurations of the VM. Do not install "Network Manager" package. The VM relies on manual/delicate configurations to provide the firewall functionalities. You may have to reinstall the VM if some configuration gets broken.
- **All parts of the solution code must be your own; copying someone else's code snippet is strictly prohibited.**
- Do not share your code with anyone, other than your project partner.
- Do not post any project-specific questions on Internet forums other than Piazza.
- The project is led by Anurag Khandelwal (main), Shoumik Palkar, and Sangjin Han. Avoid asking other GSIs project-specific questions.