Computer and Network Security

COMP-5370/-6370/-6376

Homework #2

Overview

This homework is due **22Sept2020 at 1800 CT** and you may choose to use your "late days" as discussed in the syllabus. The final deadline is 25Sept2020 at 1800CT (using all three) and any submission afterwards will be a zero (0). If you choose to use a late day, you must alert the TA of that fact *before* the deadline.

Problem 1: Secure Network Architecture

In the problems below, you will be asked to play the role of a network architect in a specific context and with a specific set of requirements. You are **not** being asked to threat model the scenario, only to implement the necessary network configurations and protections described. You **may not** make any non-standard assumptions[*] nor re-scope the scenario. If you are unsure whether something is a reasonable assumption, you may ask via Piazza[†].

Learning On-Your-Own You will need to investigate and learn small amounts of specific but well-known information on-your-own in order to complete these problems. This includes things like "What are the common ports used by Protocol X?", "What are the capabilities of Tool Y?", etc.. You *are not* expected to become an expert in any of these areas. A small amount of time (order 5–10 minutes on average) skimming documentation, blog-posts, quick-starts, tutorials, etc. is expected to be sufficient for any specific question. The ability to efficiently search, skim, and find answers to specific network and/or security-related questions is invaluable in industry. In addition to developing/practicing this skill, you should also keep any eye on what sources you are using repeatedly and remember to start there in the future.

What to Submit For both problems, you will submit three files:

- `problem-1-X.arch.png` — This is a logical network diagram of the architecture you decide is most appropriate. It must be a PNG image and **can not** be a hand-drawn representation. Be sure to label the important parts such as network devices, interconnects, subnets, important IPs, and the like.

- `problem-1.X.firewall.txt` — This is a list of `iptables` firewall rules that enforce what you determine to be the best network policy for the situation. There are numerous sources available online for how to use iptables (Wikipedia, man iptables, Ubuntu post, . . .). This should be a flat, ascii-only file. If you decide that the correct policy is no-policy, you may submit an empty file but that is *highly* recommended against.

- `problem-1-X.desc.txt` — This is a description of your network architecture that **supplements** your firewall policy and your diagram. This is an opportunity to explain details which are either too

[*] Standard assumptions are those that are unquestionably reasonable in the given scenario such as "a firewall properly implements its policy" or "BitTorrent is not a tool appropriate for the standard corporate setting".

[†] It is worth pointing out that if you are unsure about it and are unable to reassure yourself with a small amount of searching/reading online, it is most likely not a standard assumption.

abstract or complicated to represent in the other files. It must be a flat, ascii-only file and must be less than 500 words[‡].

Problem 1.1: Home Network

You (Security Sally) are a standard college student moving into a house with three other CSSE students (Alice, Bob, and Paranoid Pete) during the academic school year. As the resident security expert, your roommates have elected you to configure the all-important connection to the Internet. Your last-mile ISP has been running short on equipment so instead of their all-in-one home appliance, they provide you with:

- A basic cable modem (coax → ethernet).
- A wireless router with OpenWrt installed in its default configuration.
- A netgate SG1100 running the standard pfsense firewall software.
- A $100 gift card to "buy anything else you need for your home network".
  - They don't require receipts and don't ask for justification.

During your first supper with your new roommates, you all talk through what they want from the network you're in charge of setting up. Because you are such an excellent security-persons, you explain various S&P concepts to them such as network partitioning, wireless packet sniffing, and firewalls. At the end of it, you come up with a set of parameters for how the network should be configured and operate:

- You are the only person trustworthy enough to design and configure it in a fair and honest way (which you will).
- Everyone agrees that the gift card should be spent on *ice-cold beverages* if at all possible but understands if it's needed elsewhere.
- No one thinks that they'll need to "call into" your home network for any reason.
- It should support all major OSes (Linux, macOS, and Windows) as well as common but non-laptop clients (e.g., Raspberry Pis, gaming consoles, etc.).
- Everyone is really worried about this "Aircrack-ng" thing that you mentioned hearing about because your four next-door neighbors are all named "Mallory" or "Eve".
- Alice wants wireless and wired connections but no one else cares about having wired access.
- Bob is extremely worried about other people exhausting all the bandwidth for the month in the first two weeks.
- You are really worried about your ISP collecting and selling you and your roommates' web traffic.
  - You keep hearing people on YouTube people talking about some "ZPM" they rush the ad-spot through too fast to understand them but were able to write down all of the "free trial month" discount codes.
- Paranoid Pete is far too paranoid to let you setup, configure, or install anything on his devices more complex than the wireless network and its password.

[‡] The `wc` bash command will be useful in this regard.

Problem 1.2: Small-Office Network

You have been charged with designing and building new satellite office network for a small regional office supply company. With the exception of fetching certain information from Corporate (described below), this office operates as an independent entity including running its own web servers, clients, and network infrastructure. The CFO does not understand security and has only approved the purchase of a single, 2-port iptables-based firewall. You have access to multiple switches and routers but they are only capable of the most basic functions (i.e. switching or routing).

- Your network has been assigned the net-block of `1.1.1.1/24`.
- Corporate uses the net-block is `175.45.176.0/24`.

The corporate has handed down the parameters for your network after consultation with Council of Security Elders and Kompliance Karen but it's up to you to figure out how to make it a reality. You must meet all the parameters and impress them with your understanding of secure network architecture to have a chance of joining the Council. Their requirements are:

- All employees must be able to use the Internet in a relatively normal fashion to accomplish normal tasks in corporate environment.
  - Browsing the Internet, sending/receiving email, VoIP calls over TLS protected SIP, etc.
- You must run your own mail server internally and be able to receive email from clients.
- You must run your own web servers but all of your content must be served via the Cloudflare CDN's reverse proxy mechanism (i.e. your servers are the "origin servers").
- Your own web servers must not be accessible by anyone on the Internet other than Cloudflare.
- The office manager must be able to obtain the most up-to-date price lists from corporate at all times.
  - Corporate serves these via an active FTP server that they host.

Problem 2: Analyzing Network Traffic

Attackers and defenders both frequently study network traffic to search for weaknesses, extract otherwise difficult to obtain information, or to characterize typical network behavior. For the below problems, you will accustom yourself with the Wireshark network analyzer which is the standard tool for these types of endeavours. If you have never used Wireshark before, there are numerous tutorials and guides available on the Internet but the most complete source is the Wireshark User's Guide. Wireshark can run on all major OSes through either compiling the source-code, downloadable binaries for Windows and macOS, or OS-specific package managers.

Problem 2.1: TLS Handshake (browser)

Using a common browser of your choosing (Firefox, Chrome, etc), capture a single TLS connection to https://problem2-1.hw2.comp5370.org and store it as a pcap file named `problem-2-1.pcapng`. Based only on the TLS connection in that pcap, answer the following questions:

- **Question #1** — What TLS version was used?
- **Question #2** — What cipher suites did the client offer?
- **Question #3** — What block cipher did the server select?

- **Question #4** — What cipher mode did the server select?
- **Question #5** — What key exchange algorithm did the server select?
- **Question #6** — What MAC algorithm did the server select?
- **Question #7** — Of the TLS extensions offered by the client, select three (3). For each, give a 1 sentence of what it means in the context of or as it changes the TLS handshake. It is **not** sufficient to simply describe the Wireshark output. You should take some time and read-up on its documentation in order to adequately answer this question.

Problem 2.2: TLS Handshake (non-browser)

Repeat the actions for Problem 2.1 using the filename `problem-2-2.pcapng` and the server at https://problem2-2.hw2.comp5370.org with a non-browser TLS client[§]. Based only on the TLS connection in that pcap, answer the following questions:

- **Question #1** — What TLS version was used?
- **Question #2** — What cipher suites did the client offer?
- **Question #3** — What block cipher did the server select?
- **Question #4** — What cipher mode did the server select?
- **Question #5** — What key exchange algorithm did the server select?
- **Question #6** — What MAC algorithm did the server select?
- **Question #7** — Of the TLS extensions offered by the client, select three (3) **other than those selected in Problem 2.1**. For each, give a 1 sentence of what it means in the context of or as it changes the TLS handshake. It is **not** sufficient to simply describe the Wireshark output. You should take some time and read-up on its documentation in order to adequately answer this question.
- **Question #8** — What command did you use to fetch the URL?
- **Question #9** — Are there any notable differences between the two clients? If so, are there any security implications?

What to Submit

PCAP Files For problems 2.1 and 2.2, submit separate pcap files containing **only** the TCP flow for that specific instance with the filename given. You can extract a single TCP flow from a larger pcap by:

- Locate the TLS handshake you wish to extract
- Right-click one of the packets and select “Follow” → “TCP Stream”
- Close or ignore the pop-up stream window and return to the standard window
- Review the packets to ensure that only the intended information is shown
- Click “File” → “Save as” and enter the appropriate filename
- You can verify that only the intended packets are included by closing Wireshark entirely and opening with the given file.

[§] Such as `curl`, `wget`, `openssl s_client`, etc

Answer Files Responses to the questions listed must be in a flat, ascii-only text file named `problem-2-responses.txt` and formatted as listed below. Failure to submit an flat, ascii-only text file will result in a deduction of 10 points from your grade for this homework.

```
# Problem 2.1

Date/Time:
The date and time the connection was made

Client Implementation:
The client and version used to create the connection

Question #1:
Response to Question #1

Question #2:
Response to Question #2

...

Question #7:
Response to Question #7

# Problem 2.2

Date/Time:
The date and time the connection was made

Client Implementation:
The client and version used to create the connection

Question #1:
Response to Question #1

Question #2:
Response to Question #2

...

Question #9:
Response to Question #9
```