Assignment 3: Hacking challenge (10%)

CPSC 329 – Fall 2024

Due at 23:59, Nov. 27 on Gradescope

Assignment policy:

- This is an **individual** assignment, so the work you hand in must be your own. Any external sources used must be properly cited (see below).
- Submit your document as a **single PDF** to the correct location on Gradescope.
- Remember that you can resubmit your assignment after it has been returned with feedback. The resubmission deadline will be announced after grading is complete.
- Extensions will not be granted to individual students, so make sure you submit well before the dropbox closes. If you miss the deadline, you can submit at the resubmission deadline, but the maximum grade you can earn will be lower as a result.
- All submissions must be clearly legible. Handwritten assignments will be accepted, but marks may deducted if the TAs cannot read your writing. It is recommended that you use LaTeX or a word processor to typeset your work.
- Cite **all** sources for material you hand in that is not your original work. This includes any articles you read as part of the assignment description and tools (such as NMAP) that you used to complete it. Citations should be in a standard format such as IEEE.
- Citing sources avoids accusations of plagiarism and penalties for academic misconduct. However, you may still get a low grade if you submit work that is not primarily your own. Remember, if you are having trouble with an assignment, it is always better to go to your TA and/or instructor to get help than it is to plagiarize.
- Discuss and share ideas with other students as much as you like, but make sure that when you write your assignment, it is your own work. A good rule of thumb is to wait 20 minutes after talking with somebody before writing it down. If you exchange written material with another student, take notes while discussing with a fellow student, or copy from another person's screen, then this work is not yours.

Mission briefing:

The year is 2077, and the world has fallen into disarray. Society is run by a few competing megacorporations that control the population through military force. Terror reigns, and those born outside the circles of influence have no hope for a better life.

In this world, you are a netrunner – a punk living on the fringes of society. You specialize in hacking, infiltrating, and spying through computer systems. No sooner do you make an eddie than you spend it, as life is too short to plan ahead. You live eternally caught in the less-than-legal underground schemes between the competing corporations. If you are caught on the wrong side, you won't escape alive.

Of your many targets, Arasaka poses the greatest challenge. The company is foremost among the ruling megacorporations, and they have a brutal business strategy. They specialize in weapons development and mercenary services. Rumour has it that they have started work on a new top-secret weapons implant, the Cyberskeleton 2.0. If this project is successful, there will be no one who can rival Arasaka's military might. In their quest for complete power, it is clear that they would not hesitate to wipe out all of humanity in the process.

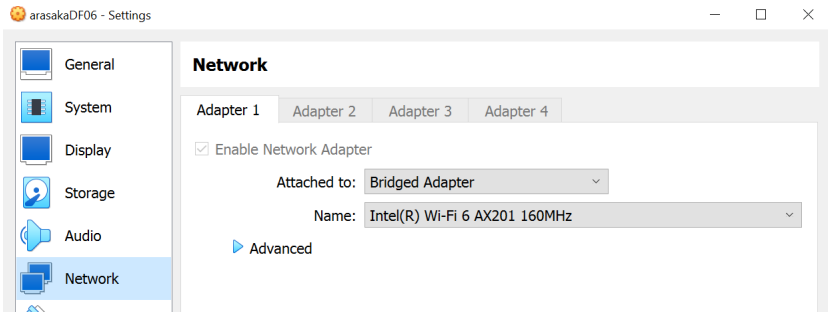
It is clear what you must do. Hack into the Arasaka servers and retrieve the research schematics for the Cyberskeleton 2.0. Many companies would pay a hefty price for the schematics, so you won't be the first netrunner to attempt this. However, you swear you will be the first to succeed. Good luck choom.

Tasks:

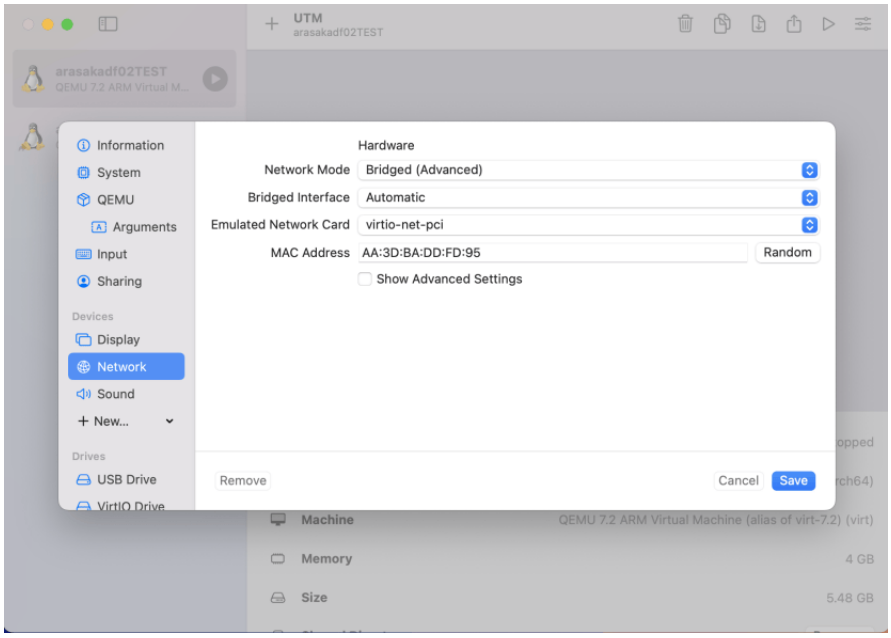
To start your mission, you easily identify the data fortress where the schematics are kept and break into the private network where it is contained. Your goal to steal the contents of the `schematics` file, which is located somewhere in the data fortress. To simulate this scenario for your assignment, you need to follow the setup below.

1. Make sure you have read all of the assignment instructions before you start.
2. Download the `arasakaDF06.ova` (VirtualBox) or `arasakaDF02.qcow2` (UTM) virtual machine file from D2L, then import and run it in your installed VMM. This is the Arasaka data fortress you must hack into for your mission.
3. Make sure your network settings for the server are set to "bridged". This will make sure that the data server appears on the same private network as the computer you run it from, so if you are trying the assignment on your home network it should appear as a separate device in that subnet. This will simulate having network access to the server. If you are not sure how to do this, ask your TA for help.

   In VirtualBox, you can find this setting after you start the VM from the top menu under Devices → Network → Network Settings, where you can set Adapter 1 to "Bridged" as shown below.



In UTM, you can do this by stopping the VM (if already open) by selecting the square stop button in the top right. You can find the window shown under Settings → Network, where you should change the network mode to "Bridged (Advanced)" as shown.



4. Your goal is to retrieve the contents of the `schematics` file. This file is located somewhere on the target server. Your job is to find it and copy it to your host computer. Make sure you include screenshot evidence with timestamps to demonstrate you have completed this task.

5. For your assignment submission, you need to create a PDF documenting your hacking process. Describe all the system vulnerabilities you found, and how you exploited them to obtain your goal. How did you figure out each step, what did you try along the way, and why? Take screenshots to illustrate as appropriate.

   Note that the majority of your assignment grade is based on how clear and professionally presented this document is (and if it is entertaining to read, all the better).

Notes:

- For the purposes of this assignment, you must hack as if you **do not have physical access** to the data server. All you should do is start the sever on your VMM – you should just minimize this window and do not directly interact with this server otherwise. All hacking should be done from your host computer. If your solution uses any actions that require physical access to the server, you will be given a grade of 0 on the assignment.
- It is strongly recommended to take notes and screenshots as you attempt the hacking. Most of the marks for the assignment are based on how well you document your thought process, regardless of whether you reach the full objective. Keep notes as you go about what your ideas are, and what you tried and why (including what didn't work!). If you got ideas or hints, make sure you document these too. If you keep good notes as you go, this will make it much easier to write up your final report afterwards.
- Everything you will need to complete the assignment has been covered in class, so focus on the basics if you get stuck. Make sure you have good notes from lectures and are up to date on your tutorial worksheets. If you are not sure what to do, focus on the Linux commands from your cheatsheet and Tin's tutorial, as well as the important files and tools we have talked through in lectures.
- If you really get stuck and need a hint, the TAs and myself are willing to guide you in the right direction. You can either come to us in person or message us privately on Piazza. Please do **not** give or ask for spoilers/hints publicly on Piazza, as we want everyone to have a fair chance to try the assignment on their own first. If you get ideas for how to proceed from anyone, including teaching staff and other students, then this must be noted in your writeup.
- If you are working on the campus WiFi, then sometimes it blocks you from locating the VM. In this case, you can use a mobile hotspot to create an isolated network where you can find the VM.
- If you don't manage to fully retrieve the target file, don't panic! You can still earn most of the marks based on how much progress you made. Write up as many vulnerabilities as you were able to exploit, and include any thoughts or ideas you had for how to continue from where you got stuck.
- If at any point you feel like you have accidentally messed up the virtual machine beyond repair (e.g. modified or deleted something you shouldn't have), you can always import a fresh copy of the `arasakaDF06.ova` or `arasakaDF02.qcow2` file and start the hacking process again from where you left off.

Grading requirements:

The assignment will be graded as follows. Four of the ten marks will be allocated for how far you get on the hacking portion (4/4 means you successfully retrieved the file, and you can get partial marks based on how far you get). If you don't make it the full way and still want these marks, we will give a hint when we return your assignment and you can try again for the resubmission deadline.

The remaining six of your marks are dependent on the quality of your report. This will be graded on our usual 0-80-100 marking scheme. Here, we are looking for how well you are able to explain your reasoning and justify the steps you took to complete the assignment.

To get full marks for this component, your responses will need to satisfy the following criteria.

- All steps are documented and well justified.
- Full thought process is explained, including ideas attempted that didn't work out and any hints received.
- Screenshots are included appropriately as evidence to show what was attempted.
- If end goal was not reached, some thoughtful ideas are presented for how to proceed.
- If end goal was reached, the file transfer is supported with screenshots as evidence.
- Assignment is cleanly formatted and easy to read, with not too many spelling/grammar/typesetting mistakes.
- References are appropriately used for all resources and citations are properly formatted.

---

author: jcleahy@ucalgary.ca