# Project Assignment

A mock corporate network has been rigged by the teachers in a virtual environment. On various places in this network, flags (jpeg images) are placed. The overall objective is to capture all the flags. There are around a dozen flags to be captured. To assist students, hints will be offered for each flag according to a schedule.

To complete the project assignment, students are free to use their imagination and tools available on the Internet. In the provided reading material, participants are introduced to specific network and vulnerability scanning tools, platforms for development of exploits, for remote control of computers, for password cracking, and so on. Nonetheless, participants are eventually free to choose methods and tools of their own.

## Starting Point

At the start of the course, hackers (students) obtain VPN credentials to connect to the virtual company's Office LAN, protected by a firewall.

## Objective: Capture the Flags

The objective of the mission is to compromise the system as fully as possible. In order to prove that they were able to hack hosts, participants need to collect **steganographic flags**: they take the form of JPG images. Collecting the flags proves that the participants have managed to hack a host.

Participants should submit the flags as soon as they collect them. Flags are named 1.jpg, 2.jpg, etc. Submissions are performed through Canvas under the Assignments *Capture Flag n.* Flag *2.jpg* should be submitted through the corresponding assignment **Capturing Flag 2 (https://kth.instructure.com/courses/5154/assignments/19816)** .

To pass the course, all flags need to be collected. The virtual worlds are closed on the final day fo the course. If, at that point, flags remain to be captured, it might be possible to prolong the life of your world for some additional days, but tardiness will affect your grades adversely.

## Hacking Log

Student groups are required to document their work in **a log submitted weekly** to teachers through Canvas. Read more about the log **here (https://kth.instructure.com/courses/5154/pages/the-hacking-log)** .

## Grading

The final grade in the project assignment will mainly depend on the aggregated value of captured flags capture, but also on hacking logs, and occasionally also on other factors (e.g. oral exam). If hacking logs and other factors are satisfactory, we aim to grade as follows:

A: 80-100% of maximum flag points
B: 60-80% of maximum flag points

C: 40-60% of maximum flag points
D: 20-40% of maximum flag points
E: 0-20% of maximum flag points

We reserve the right to update these numbers in exceptional circumstances.

For a passing grade, all mandatory assignments need to be completed, notably the hacking log.

In some cases, teachers might request that the project assignment is presented in person. This examination consists of an individual interview where teachers will be asking the student to explain and occasionally demonstrate parts of their accomplishments during the course. The oral exam is mainly aimed at determining that the student's physical self corresponds to her digital one, so we expect the ability to explain how various flags were captured, and why the employed methods were selected. If requested, the oral exam is mandatory.

# Tools

Kali Linux is suggested as a penetration testing platform. Information on how to install these tools can be found **here (https://kth.instructure.com/courses/5154/pages/kali-linux-on-virtualbox)** . Of course, it remains the participants' choice to decide which setup suits them best. However, the teachers will not be of much help if an alternative setup is not working properly, as the virtual environment has only been tested with the aforementioned setup.

# Hints

As time progresses, students will receive hints that facilitate the exploitation of the network.
Because hints reduce the difficulty of capturing flags, the value of the flags shrink with the amount of disclosed hints. For students who fail to solve a task independently within a reasonable time frame, demo videos will be made available (which will further lower that value of the associated flag).

# Support

You are encouraged to request assistance if you encounter challenges that seem beyond the intended scope of the course. For course-content-related questions, e.g., if you are uncertain about what target you should select, how to make progress in the course, what hacking methods are allowed, or where to find information, contact Pontus Johnson through Canvas.

For support with respect to the technical infrastructure, contact Teaching Assistant Nikoalos Kakouros. For instance, if you believe that a system service has become unavailable, you can request a reboot of the affected host.

Any questions that are of general interest may be mirrored to the public course discussion forum (unless you explicitly mark that communication as private). If deemed suitable, actual-reality tutoring sessions may be scheduled at KTH.

# Rules

Some rules are required in a course on ethical hacking.

- When connected to the Google Cloud virtual environment via VPN, you are **allowed to attack hosts within the network zone 10.0.0.0-10.0.15.254. If seen from a host on that network, addresses in the ranges 172.16.0.1-172.31.255.254 are also permitted targets.** All other machines are off bounds. Note that penalties for illegal hacking can be very severe (links to more information on this topic are available on the **Readings** (https://kth.instructure.com/courses/5154/pages/readings) page).
- An important part of hacking is reconnaissance, i.e. information gathering. Therefore, while we encourage sharing of general security knowledge (e.g., how does encryption work, what does the term *XSS* mean, what is a good tool for password cracking), you are not allowed to learn of network-related secrets, such as user names, passwords, IP addresses, specific vulnerabilities and exploits, or the location of flags from your fellow students. To guard against this, logs are monitored to ensure that student groups progress in a credible manner through the network. Groups with logs that e.g. do not display credible search behavior, but instead indicate prior knowledge of vulnerabilities, are flagged as suspicious. Also groups with logs that display significant similarities are flagged.
- Because you will be gaining root access to several computers, it will be possible for you to make them inoperable. However, in real-life engagements, offensive operations generally require stealth. Furthermore, disabling systems may close possible attack paths for you. Breaking the system is never required to accomplish the goal, and in general discouraged. (However, if you unintentionally do break a system, contact technical support to bring it back up again.)
- If you by happenstance were to discover a vulnerability in the Google Cloud Infrastructure, then it will be important to report it via Google's **Vulnerability Reward Program** (https://www.google.com/about/appsecurity/reward-program/). The same goes for the **Canvas LMS** (https://www.canvaslms.com/security). Additionally, such findings will count as bonus points in the course.

# The Infrastructure

The virtual network you will interact with is hosted by Google Cloud. The most important difference between this environment and a physical network, for the point of view of this course, is that OSI layer 2 is missing. Thus, ARP spoofing and other techniques based on Layer 2 won't work.

The Internet Assigned Numbers Authority (IANA) reserves the following IP address blocks for use as private IP addresses: 10.0.0.0 to 10.255.255.255. 172.16.0.0 to 172.31.255.255. 192.168.0.0 to 192.168.255.255. Note that the network address space of the virtual world is located among these. You might be used to seeing these behind a NAT, and thus unreachable from other networks. In this world, however, such assumptions cannot be made.

Furthermore, as in the case of a real corporate network, things might change in the network. Notably, systems may be restored to their unhacked state at any time, e.g. on a daily basis. Therefore, it is important to be able to repeat your hacks; thus, record your methods after successful exploitation.

# The Zen of Hacking

Some advice on how to approach the challenges you will face in this course: Hacking is not user-friendly. On the contrary, you will be walking not only unpaved roads, but roads with intentional roadblocks. Exploits typically do not work on the first attempt, and even when they work, they are often unstable. You may experience significant frustration when your hack fails to execute as intended, and more frustration

when the cause turns out to be trivial, such as a typo. The process of trial, error, analysis and correction is, however, very often excellent grounds for learning. So take the opportunity to learn. When things don't work, learn about the underlying technology as well as the tools and methods that may help you better understand the problem.