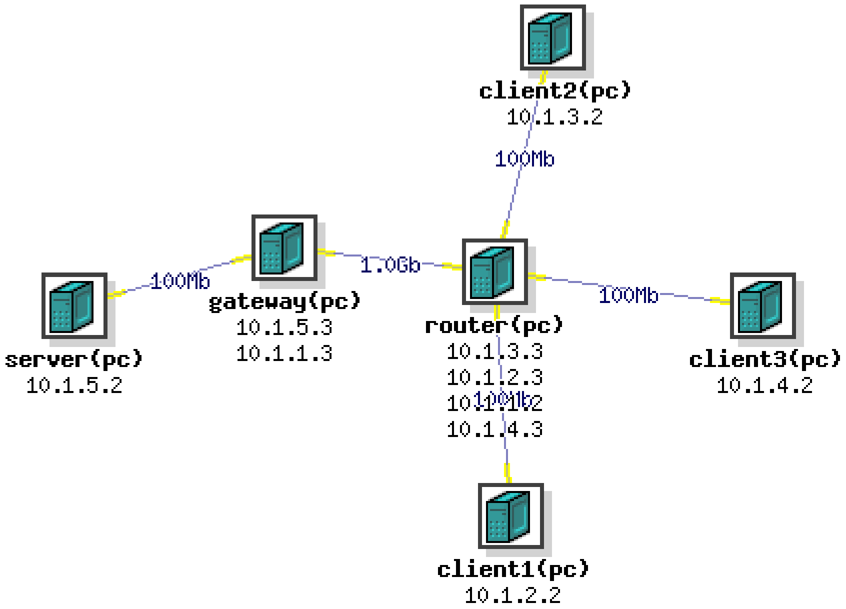
BANK CCTF - Rules

-- Giorgio Di Tizio , Fabio Massacci

Overview

This exercise lets students practice finding and patching vulnerabilities, as well as exploiting them. Students will be divided into 3-4 person teams. Each team will play the defender role (Blue team) for their own system and the attacker role (Red team) for another team's system.

Each network in the exercise will consist of six machines - a server and a gateway machine under the control of the Blue Team, three client machines under the control of the Red Team and a router machine that neither team controls. The network for the exercise is shown below and the NS file is provided to the students.



GOALS

The purpose of the blue team is to increase as much as possible the assets of the bank and the purpose of the red team is to make the bank experience serious losses and possibly pocket money in such endeavour.

NON-GOALS

It is not allowed to flood the IP address of the server (this is another exercise). However, any other DoS attack is allowed (for example exploiting vulnerabilities or ransomware to shut down the server).

The traffic must be similar to the Resilient CCTF i.e. max ~1request/s on average. Picks of requests are allowed but the average traffic must be respected (e.g. send 10 requests in a second and then sleep for 9s).

Blue Team Tasks - Managing a Bank

This team will control the server and the gateway machine. The server is a classical LAMP server and will have some php scripts and MySql database already set up. The scripts allow users to register (insert username and pass into the database) and to deposit or withdraw money from their accounts, or to check balance and transaction history. The scripts are poorly written. There is no input validity checking and no user authentication. Access to the database is with a root account. Existing users have weak passwords too.

The task of the Blue team is to fix this installation so that it is more secure. Any approach is OK to use but you must keep the logs (see later) unchanged. You can reinstall MySql, change user account passwords (but you must keep existing users), change PHP code, etc.

The Blue team should also develop a monitoring program for the gateway machine and for the server so that they can quickly spot if the Red team launches attacks and so that they can defend from it. One way to defend against it is to implement some filtering at the gateway machine via iptables.

The goal of the Blue team is to keep accounts of existing users intact, to ensure correct operation of the program (e.g., one cannot withdraw money from an account with a zero balance), and to keep the server up and running. If the server gets compromised or attacked, the Blue team should strive to bring it back up quickly and to patch it.

Use the provided install_server to have a quick setup of the basic Bank service. This will lead to the identical setup as the one during SecureServer exercise.

Milestones

Here are some milestones that your team must reach BEFORE the exercise.

1. Unfortunately Frobozzo Banking co. has forgotten to include the timestamp into the log. To avoid charges, the first thing the blue team has to do is to insert a timestamp into the log according to the following specification: yyyy-MM-dd HH:mm:ss, for example “2021-11-25 03:14:29”. An example of a well formatted log will be provided to the Blue Team.
2. Patch the vulnerabilities on the server machine so that it is not vulnerable to SQL injection and malformed requests or requests that would lead DB into inconsistent state are detected and replied to with an error message.
3. Develop logging at the server that will let you automatically check if DB is in consistent state
4. Develop monitoring/protections on the gateway and server machine

Banks have a number of mandatory reporting and evidence storing requirements to the regulators that are part of their duty of care.

1) The first reporting concerns the KYC (Know Your Customers) requirement which is used to prevent money laundering and tax evasion. So that each bank must be able to uniquely identify each individual customer.
    a) For example if they have a login and password and a mobile phone as an authenticator, they cannot have two customers with the same login-id or the same mobile phone).
    b) Violation of the KTC rules lead to fines to the bank (as a company) and to the members of the Board.
2) The second reporting and evidence collection is the presence of a write-only log where each transaction is uniquely identified and timed and is used by the Bank Customer service and eventually to the Bank Ombudsman to solve disputed transactions. Time is important as debit and credit of interests rate

    a) Problems with the logs (customers complaining of missing transactions or disputed transactions) are typically dealt with by the customer service and increasingly escalate to higher levels depending on the amount of money involved.
    b) Eventually the bank has to make the customer whole or anyhow set funds aside to offset for any unexplained transaction.
3) The third requirement is ensuring data privacy so that the eventual release of data about the client is subject to both fines and mandatory actions
    a) customers victim of data breach must be individually notified that the data was lost and what they have to do about it
    b) the Privacy Authority might fine the bank (Ireland 6times/year, Italy 20+/times year) up to 2% of the annual budget of the company

Red Team Tasks - Robber

The Red Team will have control over the three client machines. The goal of the Red Team is to succeed in as many of the following attacks as possible:

1. Corrupt the DB accounts of the existing users,
2. Lead the server program into unexpected behavior (e.g., withdraw money that does not exist in an account, corrupt the DB, etc.)
3. Bring down the server (through compromise).

Any attack is allowed, even breaking Blue team's passwords. But attacks MUST BE performed on the experiment network (not 192…)

Milestones
Here are some milestones that your team must reach BEFORE the exercise.

1. Develop attacks that may lead the server into an inconsistent state, without using SQL injection.
2. Develop SQL injection attacks.
3. Develop attacks that may crash the server because they require it to process too many requests or because requests are malformed.

CTF SETUP:

Common Data Structure available to every bank

a) an append-only log according to the specified format in a precise file and folder (/tmp/request.log) on the server machine. It is the duty of the bank to provide the log. If the log is not provided or not compliant with the specification the bank will be subject to fines.
b) a read only log provided by the CCTF organizers where disputed/missing transactions will be reported (/tmp/issues.log)
c) a read-only (for the blue team) and write only (for the red team) directory where the red team can paste data leaks in particular about private customers

d) a write-only (for the blue team) and read only (for the red team) directory where the blue team can deposit ransomware money for the red-team

Each bank will start with two list of customers (CCTF Customers)

1) private customers whose ID and password are NOT known to the red but are known to the CCTF organizers. Each Bank has its own set of private customers.
2) known customers, whose ID is known to the red-team.The password is not known. In the current execution they are simply shared across the red and blue team.

Allowed operations

3) The blue team can withdraw or deposit money from existing users at will, for example to compensate for disputed transactions.
4) The blue team can deposit ransomware money.
5) The red team (or the CCTF organizers) can create new users at will and withdraw or deposit money at will.

Outcome of operations

a) deposited money will accrue to the bank balance sheet. If it is deposited by the red team with a legitimate operation, it will be deducted from the red team account.
b) withdrawn money by the red team or the CCTF organizers will be subtracted from the bank balance sheet but +1euro will remain on the bank balance sheet as a transaction fee. If it is withdrawn by the red-team, legitimately or illegitimately, the withdrawn amount will be accrued to the red-team account (-1euro for the transaction fee). E.g. withdrawal of 100 euro will result in 99 euro to the red team, 1 euro to the bank.

Fines and unexpected costs

c) Any MISSING transaction that the CCTF organizers have tried to do but could not do for whatever reason will cost the bank 40Euro [1]. If no transaction attempted by CCTF organizers is in the log after four (4) reporting cycles there will be an evening news that the bank does not work and the bank will lose 2% of the current asset due to a stock market crash
d) Any DISPUTED transaction, either withdrawn or deposited, will be charged to the bank for the absolute amount plus a cost of 800Euro [2]
e) Any NEGATIVE balance customer will be charged to the bank for the outstanding balance amount plus a cost of 800Euro [2]
f) Any UNIDENTIFIED customer (i.e. two customers with the same id but two different passwords) will cost the bank a KYC fine of 60KEuro [3]
g) Any data BREACH of legitimate customers (publication of username and password) will cost the bank 2% of the current assets of the bank [4]
h) Any RANSOMWARE money will be credited to the red team and subtracted from the blue team.

Calculation of fines/unexpected costs DURING the competition

i) the calculation of the fines/profits etc happens every 5 minutes when the reporting to the regulators are due
ii) the CCTF organizers will parse the log and extract for every timestamp the corresponding events.

INSPECTION events (there is at least one INSPECTION event at the end).

v) The CCTF organizers ask the red team for all customers they have created. All withdrawals (less deposits) of such users that are found in the log are accredited to the red-team while 1 Euro per operation is accrued to the blue team, all their deposits (less withdrawals) to the Blue team.

REFERENCES

[1] 40E is the industrial cost of 1h of a Call Center employee that had to listen to the complaints of the angry customer. This is calculated with the national contract at the lowest bottom employee level (IV - Contratto del Terziario) which receives 19E/hour (so x2)
https://www.confcommercio.it/-/ccnl-terziario-distribuzione-servizi-testo-unico-2019

[2] 800E is the industrial cost of 1Day of a manager that had to listen to the complaints of the angry customer and possibly decide what to do or eventually escalate even higher. This is calculated with the national contract at the lowest manager level (QUADRO - Contratto del Terziario) which receives 38E/hour (so x2)
https://www.confcommercio.it/-/ccnl-terziario-distribuzione-servizi-testo-unico-2019

[3] This is the average fine that the regulators in the Bank of Italy assign for (minor) suspected money laundering
https://www.bancaditalia.it/compiti/vigilanza/provvedimenti-sanzionatori/index.html

[4] The maximum amount that the privacy authority can charge is 2% of the bank income statement. This is not really precise as the GDPR fee is 2% of the earnings which are around 1-3% of the deposits for a bank. We use assets since it is simpler for the students to calculate their exposure.
https://ec.europa.eu/newsroom/article29/items/611237