Assignment 3: AppSec

Computer and Network Security

Assistants:
Elia Geretto Brian Johannesmeyer

Q1 2020/21

Goals

- Show that you are more than just a script kiddie.
- Train and test your ability to perform file system-based, environment-based and similar local attacks.
- Train and test your ability to perform memory-based local attacks.

Task description

You are given unprivileged SSH access to a VM with 10 challenge binaries.

You should **exploit** the challenge binaries to obtain higher privileges.

Structure

The `/var/challenge/levelX` directories contain the challenges. Each of them has:

- A `setgid` binary which can be run as group `levX`.
- The source code for that binary.

You can exploit binary `X` to become a member of group `levX`.

The challenge number `X+1` is accessible only if you are a member of the group `levX`.

Tools

For your convenience, two tools are available:

- `133t`: permanently adds your user to your current group.
- `score`: shows how far everyone has progressed.

Linux caches group membership, so you may have to reconnect before `133t` takes effect.

Fair use policy

You are using a shared machine, so:

- Do not expose your solutions to others (file permissions).
- Do not attack the infrastructure, only the target programs.
- Do not overload the machine:
  - We may kill your processes and/or delete your files if they interfere with other students' access.
  - We may disable your account and/or adjust your grade in case of deliberate/repeated offenses.

Grading

Your base grade will be the number of challenges you have beaten.

The same rules as the previous assignment apply:

- A bonus based on speed (the time when you run `133t` counts).
- A malus for late submission.

Submission (1)

Deadlines and submission will be handled through Canvas.

You will find a `sanity_check.py` script on Canvas. Use it to **test** your ZIP archive before submission. If the archive does not pass the tests, your assignment will not be evaluated!

Do **not** include binaries in your archive!

Submission (2)

The archive should contain:

- `README`: Plain ASCII file containing on **separate lines**, in this sequence, with no further text:
  - Hacker handle, name, e-mail, VUnet ID, student number
- A `levelX` directory for each level beaten containing:
  - An `exploit.sh` script that runs the exploit.
  - Any source files `exploit.sh` may need.

The files should **not** be in a subdirectory.

The size should be at most 5 MB compressed and 50 MB uncompressed.

Access

You should be able to access the machine at `appsec.vusec.net`:

- Username: your VUNet ID.
- Key: The SSH key from Assignment 2.

Contact

You can ask questions through the "Discussions" page on Canvas, so that everyone can view the answer.

If you think that your question contains sensitive information, you can ask it via email to `e.geretto@vu.nl` putting `cns@vusec.net` in CC. Please, put the tag `[CNS]` in the subject.