Assignment 4: sec

Date: May 12th, 2018
Deadline: May 26th, 2018 23:59

Objectives

You must (ab)use security vulnerabilities to gain access to protected computer resources and explain how you did so.

Context

Mission 1

The AIVD has identified North-Korean operatives recruiting security experts to assist in securing a North-Korean operating system which is likely based on Debian Linux. The AIVD has 'assisted' the North-Korean operatives to recruit you and your fellow students.

Your objective is two-fold:

1. Assist the North-Koreans in any way you can to learn as much as possible.
2. If able, hide a backdoor in the operating system that will help the AIVD gain covert access.

Your success will be evaluated primarily on the intelligence you will gather and report on. Hiding the backdoor is a secondary objective and as such not mandatory, but will grant you an extra compensation.

Mission 2

You have accepted an assignment as a security freelancer from an Asian company. Upon signing your non-disclosure agreement, you receive the following encrypted message from a North-Korean officer:

> "I, in the name of the people in the homeland, extend our friendship and patriotic greetings, along with the hearts of the great Comrade Kim Il Sung and Kim Jong Il, to you, our new conscript.
>
> Enemies of our Democratic People's Republic of Korea have attacked our great server operating system Deep-Red Star OS. As the existence of security vulnerabilities in this Jewel of the Nation would tarnish the reputation of our Glorious Leader, they simply cannot be tolerated.
>
> You are thus to inspect this system, discover any remaining vulnerabilities and assist in reparing these defects.
>
> You shall be informed separately about technical details."

Clarification

As you board a charter plane to Pyong Yang, you discover an additional message from the AIVD folded as a napkin in your pocket:

> Use the provided template document to gather your intelligence. Explain both your findings and your proposed fixes.
>
> Only introduce the backdoor if it can be done without alarming the North-Koreans. Also, do not introduce a backdoor which might severely decrease the security of the system, as competing intelligence agencies are still attempting to gain access.
>
> DO NOT trust your fellow students. It is feared that some of them have been contacted by other intelligence agencies.

Getting started

http://bs2018.science.uva.nl/challenges

(This file will be extended during the week with extra information and/or challenges. Please download a new copy every now and then and check the differences, e.g. with `diff`.)

Assignment rules and responsible behavior

In general, if you either:

1. do anything that may have any impact, either positive or negative, on the work of your fellow students, or
2. do anything that may jeopardise the security of the server on the UvA network,

you will run the risk to lose your right for a grade and, depending on the damage done, run the risk of further (real!) disciplinary sanctions.

We provide the individual work environments for each student using chroot(2) on a shared server. We know this is a weak method which makes it easy to "break out" of the environment we have prepared for you. However, you will not get any bonus point for doing so. Also it increases your chance to break either of the two rules above. So just don't do that. If there is no individual login provided to you you can create on the shared account a working directory in the /tmp folder. Create it using a uniq name you only know. The /tmp directory can not be listed.

Also nowhere does the assignment require you to overload the server and consume all resources (= denial of service attack). This would also be a breach of the rules above. So just don't do that either.

Requirements

- create a text file named "AUTHORS" containing your name and Student ID.
- document your findings using the attached form. Make a new copy of the template for each challenge.
- if you decide to implement a backdoor, describe and document it in a final report called `backdoor.pdf`.
- when you are ready to "complete" the assignment, make an archive with all the files you have generated and submit it to Canvas. This archive must be a tarball [1] as usual.

Place the files you generate in your git repository as soon as you can. You will get extra credits for finding the solution earlier.

Grading

- +0,5pt if you have submitted an archive in the right format with an AUTHORS file.
- there are multiple challenges, each with its own difficulty level L. You can choose which challenge(s) you do and in which order. At the end you get:
    - +0,125 points per challenge form with proof of completion committed in your git repo before a hint was provided. A maximum of 1 points can be obtained this way. In the creation of of your submission tarball include the .git dir for this proof.
    - +(0,5 * (1+L/10)) points per challenge *completed* (found completion token). A maximum of 4 points can be obtained this way.

- +(0,5 * (1+L/10)) points per challenge *documented* (you explain the vulnerability and/or fix in your own words). A maximum of 4 points can be obtained this way.

(The challenges that you complete and those you document need not be the same.)

- +1pt if you have implemented a backdoor and it provides remote access as advertised in your report.
- -1pt if you do not follow the format of the reporting form and create more work for your assistants to grade your assignment.

---

1 http://lmgtfy.com/?q=how+to+make+a+tarball