Workshop in Information Security – Homework #5

Description:

This is the final stage of our workshop!

We will use the infrastructure we created during the previous stages and will protect against real world attacks.

IPS – Intrusion Prevention System:

Write a protection against a vulnerability, coming from the external network. Use Metasploit (exist in Kali Linux distribution, can be installed over other distributions like Ubuntu) to run the exploit and to check if your protection indeed blocks the attack.

I prepared an Excel file (attached) with a list of vulnerabilities. All of them has Metasploit module, most of them are open source.

Research the vulnerability first. You can based on published articles, the source code and the patch for this vulnerability, Metasploit module code etc.

Then write the best protection you can **without making false-positive**.

DLP – Data Leak Prevention:

Detect C code going from internal network towards outside.

Understand what is the best way to separate between sensitive C code to text.

Block outgoing C code over ports 25 (SMTP) and 80 (HTTP).

Presentation:

Prepare a presentation to explain your project. Split is into 2 or 3 parts.

1. IPS: Explain your research; what is the attack? How it works? How they fixed it? How can I determine it in the network level? How I blocked this attack? Other possible ways? What the pros, and cons.? Etc.
2. DLP: Explain your way to detect C code.
3. [Optional]: If you think you did something notable during the workshop, mention it here

Make it in way you could show it in ~10 minutes.

Submission

Prepare a ZIP file, contains:

- “module” folder, includes hw5secws.c file (the module) and the Makefile

- "user" folder, includes the user-space program and (if needed) the Makefile
- The presentation
- Other needed folders

General rules for submission:

- Document your code
- If you use a code from the internet, document it and add the source
- Individual submission
- If needed, split the files into a modular files

Good luck!

