Welcome to

4. Network Attacks and Advanced Vulnerabilities

KEA Kompetence Penetration Testing 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse 🐦

Slides are available as PDF, kramse@Github

4-network-attacks-and-adv-vulns.tex in the repo security-courses

Plan for today

Subjects
- Network Attacks and Advanced Vulnerabilities

Exercises
- From the book mostly

Reading Curriculum:
- Grayhat chapters 12-14

Reading Related resources:
- *Return-Oriented Programming:Systems, Languages, and Applications*
- *Removing ROP Gadgets from OpenBSD*

We will also revisit slide show 3-network-spoofing-password-cracking, specifically quick go through of development of wireless security WEP, WPA, WPA2, WPS problems - and relation to cracking secrets

Goals for today

.

Take a slow day

Explain in detail buffer overflows, and some of the parts

Go through examples from the book

Reproduce the parts we can

Redo buffer overflow on ARM, Raspberry Pi

Go through the OpenBSD paper and see how one operating system has decided to handle this
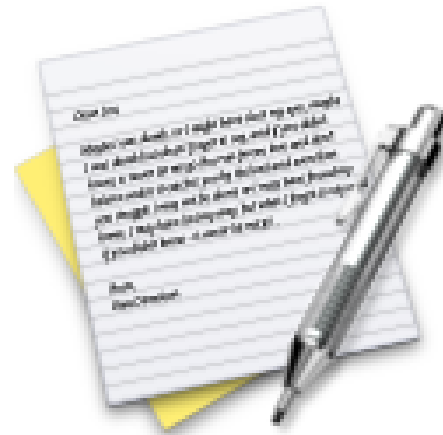
Catch up

slide show 3-network-spoofing-password-cracking, specifically quick go through:

Development of wireless security WEP, WPA, WPA2, WPS problems

Cracking secrets

Exercise

Now lets do the exercise

Aircrack-ng 30 min

which is number **19** in the exercise PDF.

Exploit components

We will dive into the book: Grayhat chapters 12-14

We need to understand the parts of exploiting

Difference between the oldest, most simple stack based overflows

The parts of a shell code running system calls

How to avoid having shell code - return into libc, calling functions

This will teach us why modern operating systems have multiple methods designed to remove each case of exploiting

Allow us to understand the next subject, Return-Oriented Programming (ROP)

Return-Oriented Programming (ROP)

We will no look into Return-Oriented Programming (ROP) hopefully prepared by the chapters for today, and exercises

Return-Oriented Programming:Systems, Languages, and Applications Ryan Roemer, Erik Buchanan, Hovav Shacam and Stefan Savage University of California, San Diego
`https://hovav.net/ucsd/dist/rop.pdf`

Them we will look into how a security oriented operating system has decided to prevent this method:

Removing ROP Gadgets from OpenBSD Todd Mortimer
`https://www.openbsd.org/papers/asiabsdcon2019-rop-paper.pdf`

Setup the OWASP Juice Shop

If we have too much time, we will look into running the OWASP Juice Shop

This is an application which is modern AND designed to have security flaws.

Read more about this project at: `https://www2.owasp.org/www-project-juice-shop/` and `https://github.com/bkimminich/juice-shop`

It is recommended to buy the Pwning OWASP Juice Shop Official companion guide to the OWASP Juice Shop from https://leanpub.com/juice-shop - suggested price USD 5.99. Alternatively read online at https://pwning.owasp-juice.shop/

Sometimes the best method is running the Docker version

Next time we will start hacking this awesome application

For Next Time
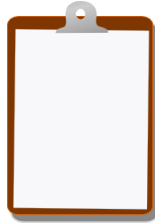
Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books
Most days have less than 100 pages, but some days may have more!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools