Lecture Network Security
Assignment Sheet 2

Jens Tölle, Wolfgang Moll
Jonathan Chapman, Martin Clauß, Martin Lambertz, Christian Meier

Summer Term 2016

Publication date of this sheet:	28.04.2016
Submission deadline (via email):	10.05.2016, 23:59:59
Discussion of results:	12.05.2016

Results must be submitted in one archive file named after the scheme
`sheet2_lastname1_lastname2[_lastname3].{tar|tar.gz|tgz|zip}`

Task 2.1 (theoretical): glibc exploit

The vulnerability with the CVE (Common Vulnerability Enumeration) identifier CVE-2015-7547 had a large impact on the security of Linux servers worldwide. Describe the vulnerability and how the exploit works conceptually. Briefly explain what NX (No eXecute, non-executable stack) and ASLR (Address Space Layout Randomization) are and how they work.

Links

- `https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2015-7547`

Task 2.2 (theoretical): Recent vulnerabilities, attacks or breaches

Briefly describe another recent network-related vulnerability, attack or breach of your choice on a technical level and answer the following questions:

- What/who is/was affected?
- Are you affected (if so, how did you react)?
- May the university be affected?
- Which sources of information have you chosen and what do you think about the quality of the sources?

Task 2.3 (practical): Website Login credentials

Future slides and assignment sheets will be available on our website. For security reasons only authorized people will have access. Therefore, the download section is protected by user name and password using HTTP basic access authentication. The current credentials with the user name `netsec_temp` can only be used for 2 more weeks. The content of our webserver's `.htpasswd` is the following:

```
netsec_temp:$apr1$XBN4ZxSl$QmLxCs3OMxZJkw7j8eVpp1
netsec:$apr1$/pE9u4cQ$ZfQfXfZ8NWh2gfFpIx22T0
```

Find out what this file does, how it works and how you can use it to retrieve the password for the user `netsec`. Crack the passwor so tha you can login as user `netsec`. Submit the correct password and the source code you used for cracking it.

Hints

- The correct password is a single word that is contained in the document "RFC 3093", which is available at `https://tools.ietf.org/html/rfc3093`.

Task 2.4 (theoretical): Password Complexity

We'll have another look at password cracking. When trying to crack a password, there are two basic ways to get candidate passwords: *dictionary attacks* and *brute-force attacks.*

Dictionary attacks (also called word list attacks) use a list of candidate passwords that are tried sequentially, whereas in brute-force attacks, all possible combinations out of a set of characters are tested. You basically did a dictionary attack on the website password, with the RFC document being your dictionary.

Part a) Dictionary Attacks

1. Search online for the "RockYou word list". What is it? Where does it come from? Do you think it is a suitable list to crack real-life passwords?
2. What do we learn about how most users picked their password?
3. How would you define "weak" and "strong" passwords in general? Why?
4. Optional question: Is your favorite password in the list? ☺

Part b) Brute-Force Attacks

Given a password length n and the disjunct character sets U, L, D, and S representing upper and lower case letters, digits, and special characters. Use the length n and the cardinalities of the character sets (e.g. $|U|$) to derive the number of possible passwords.

What causes the number of possible passwords to grow faster? Increasing n or the cardinality of the available password character set P, e.g.

$$P = U \cup L \text{ vs. } P = U \cup L \cup D \cup S$$

Task 2.5 (theoretical): PCAP Analysis #1

There is a PCAP file on the website of the lecture. Download the file and answer the following questions:

- What kind of data is contained in the trace file?
- The trace file contains an attack. What is the target?
- Please give an overall sketch of the attacker's actions.
- What is the exploit vector, i.e. what weakness is targeted by the attack?
- By analyzing the trace file, would you say this attack ultimately compromises the victim system or would you expect further steps?
- Was the attack successful?
- Can you find information about related attack methods on the Internet?
- How can you secure a system against these kind of attacks?