Assignment 2

Abbas Khan , Mariya Rybalka , Linara Adilova

May 3, 2016

Task 2.1 (theoretical): glibc exploit

The vulnerability CVE- 2015-7547 was in glibc library. GNU C Library glibc, is a library of commonly-used functions for software written in the C language to run in Linux. Its "getaddrinfo()" function is used by the client side DNS resolver, a service that translates human-friendly websites names into computer-friendly network addresses.
When making a DNS request, getaddrinfo() allocates 2048 bytes of memory for the answer, but does not check that the answer it receives fits in that buffer. The buffer overflow occurs in the function send_dg (UDP) and send_vc (TCP) for the NSS module libnss_dns when calling getaddrinfo with AF_UNSPEC family and in some cases also with AF_INET6 before the fix in commit 8479f23a.
A malicious DNS server or a man-in-the-middle attacker could provide a DNS answer that is larger than 2048 bytes, overflowing the buffer and potentially allowing the attacker to execute malicious commands.

NX(no execute)

AMD's NX bit, which stands for no execute, is a technology used in CPU's to separate memory areas for use by code and data.If the memory section has the NX attribute, this means that no processor instructions can be executed there.i.e An attacker who launches a buffer overflow attack to change the "return address" to point to his malware code stored in the data area of the memory will be defeated by a set NX attribute on the respective memory because it will not allow code in the memory area to be executed.

Address space layout randomization (ASLR)

Address space layout randomization (ASLR) is a computer security technique involved in protection from buffer overflow attacks. In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, ASLR randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap and libraries.i.e In case of buffer overflows the return addresses were overwritten with addresses that were known to be stable.
However, when an application has ASLR enabled on its binary, attempts to redirect execution flow into stack-based shellcode via a hard-coded address is likely to fail,because the location in memory of the stack buffer in question will be randomized, and guessing it would be potluck.

Task 2.3 (practical): Website Login credentials

htpasswd is used to create and update the flat-files used to store usernames and password for basic authentication of HTTP users. htpasswd encrypts passwords using either bcrypt, a version of MD5 modified for Apache, SHA1, or the

system's crypt() routine. Files managed by htpasswd may contain a mixture of different encoding types of passwords; some user records may have bcrypt or MD5-encrypted passwords while others in the same file may have passwords encrypted with crypt().
The format of file is username:encrypted password.The result of MD5 encryption has following format: "$apr1$" + the result of an Apache-specific algorithm using an iterated (1,000 times) MD5 digest of various combinations of a random 32-bit salt and the password. In our case the method of encryption used was MD5 as indicated by $apr1$ at the start. The salt for an MD5 password is between $apr1$ and the following $. In our case the salt was "/pE9u4cQ". The validity of these conclusions could be easily checked by encrypting known password and checking the result. Than, having in mind, that the new password was taken from the specific text, one could just go word by word and encrypt every one of them and compare to the cypher in the file.