Pim Trouerbach

3/12/16

Cyber-Security Midterm

Question 1: A Transposition cipher is a cipher where the order of the characters are changed but none of the actual letters themselves will be changed. A substitution cipher on the other hand is where every character is offset by a certain amount like a Caesar cipher.

Transposition Cipher: You would unravel the scroll and you would get a unreadable message

| | | | | |

| H | E | L | P | M |

| E | I | A | M | U |

| N | D | E | R | A |

| T | T | A | C | K |

Substitution Cipher:

Key = Cybersecurity

Offset each letter by 5 to get: Hdgjwxjhzwnyd

Question 2: The assembly code contains an if else statement because it has two jumps in the end of the code so one can assume that there is an if else or at least two if statements. Looking further we see that there is only one compare instruction so it can now be assumed that there is only one if statement and right after there is a jump so that it the jump to the else statement.

Question 3: I would try something like, “SELECT \* FROM Users WHERE UserId = 105 or ‘1’=’1’ #” It will evaluate the first instruction and find all users where the userId is 105 but then it will go to the second condition, the 1=1 and it will evaluate to true so it will list all users if it works accordingly

Question 4: If you look at the robots.txt you will come across a secret folder that is supposedly blocked but if you try to access it you will come to a blank page. If you look at the source of the site, you will see the password for Natas4.

Question 5: If you change where you redirect from, using a tool such as Refcontrols or burp suite you can trick the server into thinking that you are coming from natas5 so it will list the password for natas5.

Question 6: If you put a period in the query it will let you search all directories, so if you input: ./etc/natas\_webpass/natas11 it will list the password

Question 7: If you decipher what the is encrypted and you input that as your cookie you will get a password for the next level. To decipher the encrypted text you run all the operations but backwards and the opposite to get the original string. None of the functions that are used only go one way so it made this quite easy.

Question 8: Natas15 will check to see if there is a user called Natas16 then it will check the wildcard % and the command of like binary will check which characters are uppercase and which are lowercase.

Question 9:

* Strings: the strings program will list all strings in a program that are over three characters in length. This can be very helpful if a file isn’t obfuscated
* Ltrace: Ltrace runs the program that it is given and intercepts and records the calls to libraries that are in the program. It will show you step by step what the program is doing because it will output all the function calls while the program is running
* IDApro: IDApro is characterized as the best dissembler for malware, it neatly lists all the function calls and shows the control flow of program in assembly. It is helpful because you can organize the code to what you think it is doing and you change variable names and add comments to pieces. If done properly one can figure out what the piece of malware is doing as if they are looking at the source code.
* Dependency walker: Dependency walker shows all the libraries that re used and the various modules that a program is using. With this you can see what functions are being imported and you can get a rough idea for what the program is doing.
* Netcat: netcat is a networking tool for reading and writing packets to networks connections using either TCP or UDP. It can be used as a back end to listen to packets that are coming in from a server. It also has features for port scanning and port listening.

Question 10: Stored XSS attacks are much more dangerous and prevalent because they are stored at a specific page and everyone who visits the site will have the attack executed on their system. A reflected XSS attack on the other hand requires that the victim clicks on a link and the victim will then have the script directly ran on their system. While reflected XSS attacks to require that the victim clicks on a link, stored XSS attacks do not require anything from the victim, only that they are trying to visit that site that has the stored XSS attack.