Kang-Wei Chang

Kwc305

N18515255

Homework #2 - CS6823 - Network Security

1. [4 pts] What are one legitimate and one illegal use of proxies?

A common use for proxy is the proxy server which store the web content for user, which can reduce the repeat data flow on internet.

An illegal use is hacker sometimes might use proxy to hide its own IP and use multiple proxy to do the attack.

1. [4 pts] What’s the difference between netcat client and listen mode?

The client modes initial a network connection from a local system to a specified remote network port.

The listen mode is waiting the data from the network, in the command, can use –I represent listen mode.

1. [6 pts] Explain three uses for netcat and the commands required to do each one.

To do the file transfer: nc –I –p <listening port> <filename>, nc <host IP> -p <listening port> <filename>

Use the UDP protocol: server: nc -4 –u –I <port>/ client: nc -4 –u localhost <port>

To scan TCP port: nc –v –n –z –w1 <target IP> <port range> /-v: run on linux –vv run on windows, -n: not resolving names, -z: not send any data,-w1: while scanning, wait for 1 second.

1. [6 pts] Explain the three functions that covert\_tcp can do.

Covert\_tcp allows messages hidden within legitimated TCP channel and transmit without being detected . Three different functions are sending any type of raw data through 1. IP ID field, 2. TCP packet sequence number.

And 3 is to use TCP packet sequence number but send the message to a third host and spoof the source IP to the receiver’s IP to let a third host passes on the message.

1. [4 pts] Explain what Loki2 can do.

It is a type of cover program that installed on the compromised host to forge data into normal ICMP packets or UDP packets. Which are usually ignored by many antivirus scan.

1. [2 pts] In what cases is Reverse WWW Shell useful?

Because it’s allowed by firewall and anti-virus scan, it use HTTP protocol to hide its illegal data transfer.

1. [8 pts] What’s the difference between:
   1. Plaintext vs. Ciphertext
   2. Encryption vs. Decryption
   3. Symmetric Key Cryptography vs. Asymmetric Key Cryptography
   4. Encryption Algorithm vs. Encryption Key

a. Plaintext is readable text, while ciphertext is encrypted or unreadable

b. Encryption is the process let plaintext become cipherext, while decryption is the process let cipherext become plaintext.

c. Symmetric Key is involves the use of only one key.

Asymmetric key is built in pair or multiple that the key for decryption is different from the key for encryption.

d. Encryption algorithm is the method to encrypt information and encryption key is the critical part needed to do encryption or decryption. Algorithm for encryption is well known, only “keys” are secret

1. [6 pts] Describe Cipher-text only attack, Known-plaintext attack, and Chosen-plaintext attack.

Cipher-text only attack: Only the encrypted cipher text is known by the attacker.   
Known-plaintext attack: Both plaintext and cipher text are known by the attacker, but the attacker  does not know the exact correlation between plaintext and cipher text.   
Chosen-plaintext attack: The attacker knows the cipher text with corresponding plaintext that was  chosen.

1. [4 pts] Explain the purpose of a salt in relation to a password file.

Because the system store account and password information with hash functions, known as rainbow table. If every time a user has logged on, the system generate the same hash code and store in it rainbow table. The attacker knows it was the same user. In order to illude attacker from cracking the password using this pattern, the system concatenate something random in the information before generating hash codes. This something random knowns as “salt”.

1. [4 pts] Describe **one benefit** and **one problem** with stream ciphers.

Stream cipher is faster than block cipher and consume less memory. The downside is that stream cipher is vulnerable to known plaintext attack because the cipher is often predictable.

1. [4 pts] Encrypt “NETSEC” with a Julius Caesar’s Cipher of key -3 (negative 3).

KLM N  
BCD E  
QRS T  
PQR S  
BCD E  
ZAB C

KBQPBZ

1. [4 pts] Decrypt your result from the previous question to obtain the plaintext message. Show work.

Encrypt is -3, so decrypt is +3

K LMN  
B CDE  
Q RST  
P QRS  
B CDE  
Z ABC

NETSEC

Use the following mono-alphabetic cipher for the next two questions:

Plaintext: abcdefghijklmnopqrstuvwxyz

Ciphertext: mnbvcxzasdfghjklpoiuytrewq

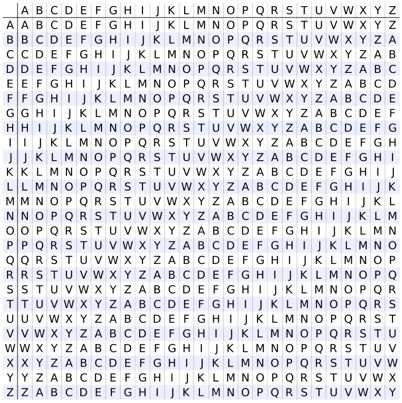
1. [4 pts] Encrypt “network”

jcurkof

1. [4 pts] Decrypt “umjvkj”

tandon

1. [6 pts] Using the Vigenère Cipher with the key “NYU”, encrypt “GREEN”. Note: on an exam, you may be ask to perform this without being given the table.



G N ->T  
R Y ->P  
E U ->Y  
E N ->R  
N Y ->L

TPYRL

1. [8 pts] Using the Vigenère Cipher, decrypt “FYOPC” using the key “NYU”.

F N ->S  
Y Y ->A  
O U ->U  
P N ->C  
C Y ->E

1. [8 pts] Compute 777 mod 17 without a calculator. Write out your calculations.

77 mod 17 = 9

77^2 mod 17 = 9\*9 mod 17 = 13

77^4 mod 17 = 13\*13 mod 17 = 16

77^6 mod 17 = 13\*16 mod 17 = 4

77^7 mod 17 = 4\*9 mod 17 = 2

Use the following block cipher scheme for rest of the questions.

**Input** **Output**

000 110

001 111

010 101

011 100

100 011

101 010

110 001

111 000

1. [4 pts] Without using Cipher Block Chaining (CBC), what’s the Ciphertext for 010110001111?

010 110 001 111

-> 101 001 111 000

1. [4 pts] Using CBC and an IV=010, what’s the Ciphertext for 010110001111?

010 110 000 000  
XOR 000 000 111 111

Cipher 110 110 000 000

Ans: 110 110 100 000

1. [6 pts] Decrypt your answer in the previous question. Show work.

110 110 000 000

Plaintext 000 000 111 111

XOR 010 110 001 111