SATHYABAMA UNIVERSITY

(Established under Section 3, UGC Act 1956)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

SCSX1026 CRYPTOGRAPHY AND NETWORK SECURITY LAB

SCSX1026 Cryptography & Network Security

EXP NO 1 SECRET KEY CRYPTOGRAPHY

AIM

To encrypt a string and then print the decrypted form of string.

ALGORITHM

Step 1: Start
Step 2: Input a string
Step 3: Convert each character of the string into its corresponding ASCII values
Step 4: To encrypt the whole string, a pre defined integer value is added to each ASCII value
Step5: The ASCII values are again converted to corresponding characters
Step 6: Hence the encrypted string is printed
Step 7: To decrypt the string, each character is converted to its corresponding ASCII codes
Step 8: The same integer value is subtracted from each ASCII value
Step 9: The ASCII value are then converted back to their corresponding characters
Step 10: The decrypted String is then printed
Step 11: Stop

Exp 2: PUBLIC KEY CRYPTOGRAPHY

AIM

To encrypt and decrypt the given plain text using RSA algorithm

ALGORITHM

GENERATION OF PUBLIC AND PRIVATE KEY

Step 1: Start
Step 2: Randomly Choose any 2 prime numbers ‘p’ and ‘q’
Step 3: Calculate’n’such that $n=p*q$
Step 4: Calculate’φ’such that $\varphi=(p-1)(q-1)$
Step 5: Pick the public key‘e’such that it is relatively prime to φ, ie gcd of$(e, \varphi)=1$

```
Step 6:    Calculate the private key ‘d’ such that’d’is relatively prime to φand a
           multiplicative inverse of ‘e’ I.e. (d*e)mod φ=1
Step 7:    Now we have the private key ‘d’and the public key ‘e’ and ‘n’
Step 8:    Stop
```

ENCRYPTION

```
Step 1:    Start
Step 2:    Input the string
Step 3:    Convert each character of the string into its corresponding ASCII values
Step 4:    Calculate the following for each ASCII values

                   $C=p^{e}mod n$
           Where,
               p = ASCII value of the plain text
               C= ASCII value of the cipher text
               e = Public Key
               n =Public Key (p*q)
Step 5:    Convert each ASCII values of the cipher text into their corresponding
           characters
Step 6:    Print the cipher text
Step 7:    Stop
```

DECRYPTION

```
Step 1:    Start
Step 2:    Input the cipher text
Step 3:    Convert each character of the cipher text into it corresponding ASCII
           values
Step 4:    Calculate the following for each ASCII values

                   $p=c^{d}mod n$
           Where,
               p = ASCII value of the plain text
               C= ASCII value of the cipher text
               d= Private Key
               n =Public Key (p*q)
Step 5:    Convert each ASCII values of the plain text into their corresponding
           characters
Step 6:    Print the plain text
Step 7:    Stop
```

EXP 3 WIRESHARK-TCP [Transmission Control Protocol]

AIM

To list out the application protocol by using TCP protocols

STEPS

I . CAPTURING THE PACKETS

a) To start capturing the packets ,click on the capture menu->option or press CTRL+k
b) Select the interface, enable packet capture in promiscuous mode, enable update the packets in real time and check the automatic scrolling in live capture.
c) Click the start button available in the dialog box

II DISPLAY FILTER SETTING

By using this, only packets matching the display filter string will be displayed in the summary window

a) By clicking the filter button in the filter bar, will display filter dialog box, where a filter string (conditions) can be provided.
b) Conditional expressions can be produced directly by typing in the text box next to the filter button in the filter bar. Click on the expression in the bar to add the condition by using the filter expression dialog box, which displays list of protocols decodes and their headers.

III SAVE THE CAPTURED TRAFFIC

You can save the captured traffic which can also be used as network based evidence.

EXERCISES

1. Draw the TCP header format?
2. Check the TCP three way hand shake?
3. Check the Value of the acknowledgement where initial SSN flag is sent?
4. Check the FIN ACK when the connection is closed?

EXP 4 WIRESHARK- UDP [USER DATAGRAM PROTOCOL]

AIM

To list out the application protocol by using UDP protocols

STEPS

I . CAPTURING THE PACKETS

a) To start capturing the packets ,click on the capture menu->option or press CTRL+k

b) Select the interface, enable packet capture in promiscuous mode, enable update the packets in real time and check the automatic scrolling in live capture.

c) Click the start button available in the dialog box

II DISPLAY FILTER SETTING

By using this, only packets matching the display filter string will be displayed in the summary window

a) By clicking the filter button in the filter bar, will display filter dialog box, where a filter string (conditions) can be provided.

b) Conditional expressions can be produced directly by typing in the text box next to the filter button in the filter bar. Click on the expression in the bar to add the condition by using the filter expression dialog box, which displays list of protocols decodes and their headers.

III SAVE THE CAPTURED TRAFFIC

You can save the captured traffic which can also be used as network based evidence.

EXERCISES

1. Draw the UDP header format.

2. List out the values of UDP packet.

EXP 5 WIRESHARK – ARP – ETHERNET

AIM

To list out the application protocol by using ARP protocols

STEPS

I . CAPTURING THE PACKETS

a) To start capturing the packets ,click on the capture menu->option or press CTRL+k
b) Select the interface, enable packet capture in promiscuous mode, enable update the packets in real time and check the automatic scrolling in live capture.
c) Click the start button available in the dialog box

II DISPLAY FILTER SETTING

By using this, only packets matching the display filter string will be displayed in the summary window

a) By clicking the filter button in the filter bar, will display filter dialog box, where a filter string (conditions) can be provided.
b) Conditional expressions can be produced directly by typing in the text box next to the filter button in the filter bar. Click on the expression in the bar to add the condition by using the filter expression dialog box, which displays list of protocols decodes and their headers.

III SAVE THE CAPTURED TRAFFIC

You can save the captured traffic which can also be used as network based evidence.

EXERCISES

1. Draw the Ethernet header format.
2. List out the values of Ethernet packet.

3. To view the ARP cache for your system open your command prompt and type arp-a.
4. Check the information column for the summary window in Ethernet?
5. Draw the IP header format.
6. List out the values ARP packet.
7. List out the values of IP Datagram.

EXP 6 WIRESHARK-ICMP

AIM

To list out the application protocol by using ICMP protocols

STEPS

I . CAPTURING THE PACKETS

a) To start capturing the packets ,click on the capture menu->option or press CTRL+k
b) Select the interface, enable packet capture in promiscuous mode, enable update the packets in real time and check the automatic scrolling in live capture.
c) Click the start button available in the dialog box

II DISPLAY FILTER SETTING

By using this,only packets matching the display filter string will be displayed in the summary window

a) By clicking the filter button in the filter bar, will display filter dialog box, where a filter string (conditions) can be provided.
b) Conditional expressions can be produced directly by typing in the text box next to the filter button in the filter bar. Click on the expression in the bar to add the condition by using the filter expression dialog box, which displays list of protocols decodes and their headers.

III SAVE THE CAPTURED TRAFFIC

You can save the captured traffic which can also be used as network based evidence.

EXERCISES

a) Identify the sequence number and identify the Ping and response packets.

b) Filter the ICMP packets and look at the destination unreachable message,Link the following.
c) List out the values of ICMP packet.

EXP 7 WIRESHARK-HYPER TEXT TRANSFER PROTOCOL

AIM

To list out the application protocol by using HTTP protocols

STEPS

I . CAPTURING THE PACKETS

a) To start capturing the packets ,click on the capture menu->option or press CTRL+k
b) Select the interface, enable packet capture in promiscuous mode, enable update the packets in real time and check the automatic scrolling in live capture.
c) Click the start button available in the dialog box

II DISPLAY FILTER SETTING

By using this, only packets matching the display filter string will be displayed in the summary window

a) By clicking the filter button in the filter bar, will display filter dialog box, where a filter string (conditions) can be provided.
b) Conditional expressions can be produced directly by typing in the text box next to the filter button in the filter bar. Click on the expression in the bar to add the condition by using the filter expression dialog box, which displays list of protocols decodes and their headers.

III SAVE THE CAPTURED TRAFFIC

You can save the captured traffic which can also be used as network based evidence.

To save the captured packets press CTRL +s and u will get the dialog box. You can save the captured packets and /or the display packets. Press save button you can later open the captured packets for analysis

EXERCISES

List out the values of HTTP packet.