

KARPAGAM ACADEMY OF HIGHER EDUCATION (Deemed University Established Under Section 3 of UGC Act 1956) Coimbatore - 641021. (For the candidates admitted from 2017 onwards) DEPARTMENT OF COMPUTER SCIECE

		Semester – V
17CSU511A	INFORMATION SECURITY - PRACTICAL	4H - 2C

Instruction Hours / week: L: 0 T: 0 P: 4 Marks: Int : 40 Ext : 60 Total: 100

- Demonstrate the use of Network tools: ping, ipconfig, ifconfig, tracert, arp, netstat, whois
- 2. Use of Password cracking tools : John the Ripper, Ophcrack. Verify the trength of passwords using these tools.
- 3. Perform encryption and decryption of Caesar cipher. Write a script for performing these operations.
- 4. Perform encryption and decryption of a Rail fence cipher. Write a script for performing these operations.
- 5. Use nmap/zenmap to analyse a remote machine.
- 6. Use Burp proxy to capture and modify the message.
- 7. Demonstrate sending of a protected word document.
- 8. Demonstrate sending of a digitally signed document.
- 9. Demonstrate sending of a protected worksheet.
- 10. Demonstrate use of steganography tools.
- 11. Demonstrate use of gpg utility for signing and encrypting purposes.

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University) (Established Under Section 3 of UGC Act 1956) Eachanari Post, Coimbatore – 641021, INDIA



(Deemed to be University) (Established Under Section 3 of UGC Act, 1956)

DEPARTMENT OF CS, CA & IT III -B.Sc. (COMPUTER SCIENCE) INFORMATION SECURITY PRACTICAL (17CSU511A)

SEMESTER: V

(2017-2020 Batch)

Name :_____

Reg.No :_____

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University) (Established Under Section 3 of UGC Act 1956) Eachanari Post, Coimbatore – 641021, INDIA



DEPARTMENT OF CS, CA & IT

CERTIFICATE

This certify bonafide done is to that this is a record work by of III-BSc. Computer Science during the period June to November-2019 for the "Information Security Practical". Examination held on _____

Reg.No:

Subject Code: 17CSU511A

Staff-in-charge

Head of the Department

(Internal Examiner)

(External Examiner)

CONTENTS

EX.NO.	DATE	TITLE	PAGE NO.	TEACHER'S SIGN
01		Network Tools		
02		Password Cracking Tool		
03		Implementation of Encryption and Decryption of a Caesar Cipher		
04		Implementation of Encryption and Decryption of Rail Fence Cipher		
05		Nmap/Zenmap		
06		Burp Proxy Tool		
07		Protected Word Document		
08		Digitally Signed Document		
09		Protected Excel Document		
10		Steganography Tool		
11		GPG Utility		

Aim:

Demonstrate the use of network tools:ping, ipconfig, ipconfig/all, truncate, arp, netstat.

Algorithm:

Step 1:Open cmd (command prompt).

- Step 2:PING IPaddress used to sends packets of data to a specific IP address on a network, and then lets us to know how long it took to transmit that data and get a response.
- Step 3: TRACERTuse to trace the path that an Internet Protocol (IP) packet takes to its destination from a source.
- Step 4:IPCONFIG tool used to find out the configured network adapters information, such as IP address, subnet mask and gateway.
- Step 5: IPCONFIG /ALL shows detailed information of network adapter that includes IP address, subnet mask, gateway, DNS, DHCP, MAC address, etc.
- Step 6: ARP maps the physical MAC address with the IP

Step 7: NETSTAT command issued to show detailed network status information.

C:\Users\User.TERMINAL90>ping 172.16.25.1

Pinging 172.16.25.1 with 32 bytes of data: Reply from 172.16.25.1: bytes=32 time=3ms TTL=127 Reply from 172.16.25.1: bytes=32 time=1ms TTL=127 Reply from 172.16.25.1: bytes=32 time=1ms TTL=127 Reply from 172.16.25.1: bytes=32 time=1ms TTL=127 Ping statistics for 172.16.25.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\Users\User.TERMINAL90>ping 172.16.4.90

Pinging 172.16.4.90 with 32 bytes of data: Reply from 172.16.4.90: bytes=32 time=5ms TTL=128 Reply from 172.16.4.90: bytes=32 time=1ms TTL=128 Reply from 172.16.4.90: bytes=32 time=1ms TTL=128 Reply from 172.16.4.90: bytes=32 time=1ms TTL=128 Ping statistics for 172.16.4.90:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\Users\User.TERMINAL90>ping 172.16.4.100

Pinging 172.16.4.100 with 32 bytes of data: Reply from 172.16.4.100: bytes=32 time=3ms TTL=128 Reply from 172.16.4.100: bytes=32 time=1ms TTL=128 Reply from 172.16.4.100: bytes=32 time=1ms TTL=128 Reply from 172.16.4.100: bytes=32 time=1ms TTL=128 Ping statistics for 172.16.4.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\Users\User.TERMINAL90>ipconfig

Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Link-local IPv6 Address : fe80::a55c:379f:a2dc:2b58%11
IPv4 Address. : 172.16.4.81
Subnet Mask : 255.255.254.0
Default Gateway : 172.16.4.254
Tunnel adapter isatap. {B49FA87C-984C-42A3-A715-EA0B95DA60C4}:
Media State : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\User.TERMINAL90>ipconfig/all

Windows IP Configuration
Host Name : Terminal81
Primary Dns Suffix :
Node Type : Hybrid
IP Routing Enabled : No
WINS Proxy Enabled : No
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Description : RealtekPCIe GBE Family Controller
Physical Address : 60-45-CB-87-3E-F8
DHCP Enabled : No
Autoconfiguration Enabled : Yes
Link-local IPv6 Address : fe80::a55c:379f:a2dc:2b58%11(Preferred)
IPv4 Address : 172.16.4.81(Preferred)
Subnet Mask : 255.255.254.0
Default Gateway : 172.16.4.254
DHCPv6 IAID : 241190347
DHCPv6 Client DUID : 00-01-00-01-21-6A-A4-B5-60-45-CB-87-3E-F8
DNS Servers : 172.16.25.8

8.8.8.8

NetBIOS over Tcpip. : Enabled

Tunnel adapter isatap.{B49FA87C-984C-42A3-A715-EA0B95DA60C4}:

Media State: Media disconnected

Connection-specific DNS Suffix . :

Description: Microsoft ISATAP Adapter

Physical Address. : 00-00-00-00-00-00-E0

DHCP Enabled. No

Autoconfiguration Enabled : Yes

C:\Users\User.TERMINAL90>tracert 172.16.4.100

Tracing route to Termina100 [172.16.4.100] over a maximum of 30 hops: 1 4 ms 1 ms 1 ms Termina100 [172.16.4.100]

Trace complete.

C:\Users\User.TERMINAL90>arp -a

Interface: 172.16.4.81 --- 0xb

Internet Address	Physical Address	Туре
172.16.4.67	b0-6e-bf-2c-1f-25	dynamic
172.16.4.75	b0-6e-bf-2c-21-a4	dynamic
172.16.4.83	b0-6e-bf-2c-1f-5b	dynamic
172.16.4.84	b0-6e-bf-2c-22-7c	dynamic
172.16.4.90	60-45-cb-86-aa-01	dynamic
172.16.4.91	b0-6e-bf-2c-25-ea	dynamic
172.16.4.94	60-45-cb-87-3f-37	dynamic
172.16.4.95	b0-6e-bf-2c-25-da	dynamic
172.16.4.96	60-45-cb-87-3e-31	dynamic
172.16.4.97	60-45-cb-87-42-ba	dynamic
172.16.4.98	60-45-cb-87-3f-b5	dynamic
172.16.4.100	b0-6e-bf-2c-22-98	dynamic
172.16.4.101	b0-6e-bf-2c-24-f0	dynamic
172.16.4.102	60-45-cb-87-3f-ba	dynamic
172.16.4.103	60-45-cb-87-49-9a	dynamic

172.16.4.104	60-45-cb-87-47-5f	dynamic
172.16.4.119	b0-6e-bf-d2-e4-2e	dynamic
172.16.4.130	b0-6e-bf-2c-1f-2a	dynamic
172.16.4.137	b0-6e-bf-2c-1f-92	dynamic
172.16.4.140	60-45-cb-87-4a-82	dynamic
172.16.4.141	b0-6e-bf-2c-1f-5e	dynamic
172.16.4.254	64-64-9b-1f-1d-41	dynamic
172.16.5.255	ff-ff-ff-ff-ff static	
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static

C:\Users\User.TERMINAL90>netstat

Active	Connections		
Proto	Local Address	Foreign Address	State
Тср	172.16.4.90:49223	maa05s04-in-f3: http	SYS-SENT

C:\Users\User.TERMINAL90>netstat -s

IPv4 Statistics	
Packets Received	= 62188
Received Header Errors	= 0
Received Address Errors	= 303
Datagrams Forwarded	= 0
Unknown Protocols Received	= 0
Received Packets Discarded	= 2195
Received Packets Delivered	= 62211
Output Requests	= 10301
Routing Discards	= 0
Discarded Output Packets	= 0
Output Packet No Route	= 0
Reassembly Required	= 0
Reassembly Successful	= 0
Reassembly Failures	= 0
Datagrams Successfully Fragm	ented $= 0$

Datagrams Failing Fragme	entation	n = 0
Fragments Created		= 0
IPv6 Statistics		
Packets Received		= 5201
Received Header Errors		= 0
Received Address Errors		= 11
Datagrams Forwarded		= 0
Unknown Protocols Receiv	ved	= 0
Received Packets Discarde	d	= 28
Received Packets Delivered	d	= 5244
Output Requests		= 187
Routing Discards		= 0
Discarded Output Packets		= 0
Output Packet No Route		= 2
Reassembly Required		= 0
Reassembly Successful		= 0
Reassembly Failures		= 0
Datagrams Successfully Fra	agment	ed = 0
Datagrams Failing Fragm	entatio	n = 0
Fragments Created		= 0
ICMPv4 Statistics		
Received	Sent	
Messages	81	81
Errors	0	0
Destination Unreachable	0	0
Time Exceeded	0	0
Parameter Problems	0	0
Source Quenches	0	0
Redirects	0	0
Echo Replies	37	44
Echos	44	37
Timestamps	0	0

Address Mask Replies	0	0
Router Solicitations	0	0
Router Advertisements	0	0
ICMPv6 Statistics		
Received	Se	ent
Messages	83	20
Errors	0	0
Destination Unreachable	0	0
Packet Too Big	0	0
Time Exceeded	0	0
Parameter Problems	0	0
Echos	0	0
Echo Replies	0	0
MLD Queries	0	0
MLD Reports	0	0
MLD Dones	0	0
Router Solicitations	0	6
Router Advertisements	0	0
Neighbor Solicitations	5	7
Neighbor Advertisements	78	7
Redirects	0	0
Router Renumberings	0	0
TCP Statistics for IPv4		
Active Opens		= 41
Passive Opens		= 776
Failed Connection Atten	npts	= 886
Reset Connections		= 28
Current Connections		= 0
Segments Received		= 43949
Segments Sent		= 8067
Segments Retransmitted		= 1772
TCP Statistics for IPv6		
Active Opens		= 0
Passive Opens		= 0

= 0
= 0
= 0
= 0
= 0
= 0
= 15918
= 2195
= 0
= 371
= 5079
= 28
= 0
= 150

C:\Users\User.TERMINAL90>netstat -e

Interface Statistics

	Received	Sent
Bytes	176974128	2534916
Unicast packets	184740	40400
Non-unicast packets	137916	1404
Discards	0	0
Errors	0	0
Unknown protocols	0	

Result:

The above program has been executed successfully and the output is verified.

Aim:

To use of password cracking tool: Join then Ripper, ophcrack. Verify the strength

Of password using these tools.

Algorithm:

Step 1:Start the process.

Step 2:Open the administrator user account id.

Step 3:In command prompt type - net user administrator *.

- Step 4:Type the password and retype the password. We get the command completed successfully and log off.
- Step 5:open command prompt type net user administrator * and change the administrator password.

Step 6:Display the result.

Step1:

C:\users\Administrator>net user

User accounts for $\underline{\TERMINAL81}$

Administrator Guest test

The command completed successfully.

Step2:

C:\users\Adiministrator>net user administrator *

The command completed successfully.

Result:

The above program has been executed successfully and the output is verified.

Caesar Cipher

Aim:

To perform encryption and decryption of a Caesar cipher. Write a script to

perform the operations.

Algorithm:

Step 1: Read the plain text from the user.

Step 2: Read the key value from the user.

Step 3: If the key is positive then encrypt the text by adding

character in the plain text.

Step 4: Else subtract the key from the plain text.

#include<stdio.h>

#include<string.h>

#include<conio.h>

#include<ctype.h>

void main()

```
{
```

char plain[10],cipher[10];

intkey,i,length;

int result;

clrscr();

```
printf("\n enter the plain text:");
```

scanf("%s",plain);

```
printf("\n enter the key value:");
```

```
scanf("%d",&key);
```

printf("\n \n \t PLAIN TEXT: %s",plain);

```
printf("\n \n \t ENCRYPED TEXT:");
```

```
for(i=0,length=strlen(plain);i<length;i++)</pre>
```

{

```
cipher[i]=plain[i]+key;
```

if(isupper(plain[i]) && (cipher[i] > 'Z'))

cipher[i]=cipher[i]-26;

```
if(islower(plain[i]) && (cipher[i]>'z'))
```

```
cipher[i]=cipher[i]-26;
printf("%c",cipher[i]);
}
printf("\n \n \t AFTER DECRYPTION:");
for(i=0;i<length;i++)
{
    plain[i]=cipher[i]-key;
    if(isupper(cipher[i]) && (plain[i]<'A'))
    plain[i]=plain[i]+26;
    if(islower(cipher[i]) && (plain[i]<'a'))
    plain[i]=plain[i]+26;
    printf("%c",plain[i]);
    }
    getch();
```

Output:

Enter the plain text: security

Enter the key value: 3

PLAIN TEXT: security

ENCRYPTED TEXT: vhfxulwb

AFTER DECRYPTION: security

Result:

The above program has been executed successfully and the output is verified.

Rail Fence Cipher

Aim:

To write a script to implement Encryption and Decryption of rail fence cipher.

Algorithm:

Step 1:Read the plain text.

- Step 2: Arrange the plain text in row columnar matrix format.
- Step 3:Now read the keyboard depending on the number of

Columns of the plain text.

- Step 4:Arrange the characters of the keyword in second order and the corresponding columns of the plain text.
- Step 5: Read the characters of row wise or column wise in the former order to get the cipher text.

```
#include<stdio.h>
```

#include<conio.h>

#include<string.h>

void main()

```
{
```

inti,j,k,l;

```
char a[20],c[20],d[20];
```

clrscr();

printf("\n\t\t RAIL FENCE TECHNIQUE");

printf("\n\nEnter the input string:");

gets(a);

l=strlen(a);

/*ciphering*/

```
for(i=0,j=0;i<l;i++)
```

{

if(i%2==0)

```
c[j++]=a[i];
```

}

```
\textit{for}(i{=}0{;}i{<}1{;}i{+}+)
```

{

if(i%2==1)

c[j++]=a[i];

}

```
c[j]='\0';
```

printf("\n Cipher text after applying rail fence:");

printf("\n%s",c);

/*Deciphering*/

if(1%2==0)

k=l/2;

else

k=(1/2)+1;

```
for(i=0,j=0;i<k;i++)
```

```
{
```

d[j]=c[i];

j=j+2;

}

```
for(i=k,j=1;i<l;i++){
```

d[j]=c[i];

j=j+2;

```
}
```

d[1]='\0';

printf("\nText after decryption:");

printf("%s",d);

getch();

}

Output:

RAIL FENCE TECHNIQUE

Enter the input string: hackers

Cipher text after applying rail fence: hcesakr

Text after decryption: hackers

Result:

The above program has been executed successfully and the output is verified.

Aim:

Use nmap/zen map to analyse a remote mechanism.

Algorithm:

- Step 1: Start the process.
- Step 2: Open nmap/zenmap tool.
- Step 3:In target address bar type the IP address 172.16.4.66 80 and Select ping scan→ scan.

Step 4: The nmap output for the ping scan is displayed on the screen.

Step 5: The ports/hosts shows the version state services for the ping Scan.

Step 6: click the Topology option,the diagram shows the connected Terminals IP address.

Step 7: using fisheye zoom option the diagram will get clearly.

Step 8: Stop the process.

Nmap output:

other Final State	can Iools Profile H	
land in the interaction intera		1
Attack Attack<	larget 172.16.4.66-80	Profile Ping scan Cancel
Attal Test Attal Test Attal Test Attal Test Attal Att	Command: nmap -sn 17.	[16.4.66-90]
Sit Heat - Provide Initial ASP -	Hotts Senice	Nimap Output Pents/Heats Teppology Host Details Scans
# 1216.00 Contring lung 1.P.((truck)/meansor) at 2016 66-31	OS + Host	• E Details
III.136.11 mot start reform in 12.13.6.4.10 III.136.12 Well defects in (12.13.6.4.10 III.136.13 Well defect in (12.13.6.4.10 III.136.14 Well defect in (12.13.6.4.10 III.136.15 Well defect in (12.13.6.4.10 III.136.16 Well defect in (12.13.6.4.10 IIII.136.16 Well defect in (12.13.6.4.1.10	I72164.70	Starting Mmap 7.70 (https://mmap.org) at 2018-08-31 09:28 India Standard Time
ITISIAT Windows: Sincers: Dirich (Lancter) ITISIAT Windows: Dirich (Lancter) ITISIATISIAT Windows: Dirich (Lancter)	172364.71	Mmap scan report for I72.16.4.70 Host is up (0.00008 latency).
1111.11 Norm of a model in the state of a model of model of a model model of a m	W 172164.72	<u>NAC Address</u> B8:66:86:26:16:19 (Asustek Computer) News reserves anost for 173 16.4.71
Interfact Microsciences 06:00:00:10:10:00:10:10:10:10:10:10:10:10:	W 17216473	Host is up (0.00008 latency).
 TD14.45 Kuister en en	W 172164.74	<u>NMC Address</u> : B0:66:86:261:05:09 (Asustek Computer) New start remort for 172.16.4.72
 TIJBAJK Weiderssi Der Gar (180-stark Computer) wir sin of 0.0006 itserv(). TIJBAJR Weiderssi Der Gar (180-stark Computer) wir sin of 0.0006 itserv(). TIJBAJR Weiderssi Der Gar (180-stark Computer) wir sin of 0.0006 itserv(). TIJBAJR Weiderssi Der Gar (180-stark Computer) wir sin of 0.0006 itserv(). TIJBAJR Weiderssi Der Gar (180-stark Computer) wir sin of 0.0006 itserv(). TIJBAJR Weiderssi Der Gar (180-stark Computer) wir sin of 0.0006 itserv(). Wirderssi Der Gar (180-stark Computer) Wirderssi Der Gar (I72164.75	Host is up (0.0000s latency).
In 1716AJT Mick Size (0) (0) (0) (0) (0) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	I72164.76	<u>MKC Address:</u> 60:45:C0:87:49:28 (Asustek Computer) Mmap scan report for 172.46.4.73
 11216.13 Web start report for 12.16.4.73 Web Start report for 12.16.4.75 Web Start report for 12.16.4.75 Web Start report for 12.16.4.75 Web Start report for 12.16.4.75 Web Start Start (12.16.4.75 Web Start Start (12.16.4.75 Web Start Start (12.16.4.77 Web Start Start (12.16.4.77) Web S	W 17216477	Host is up (8.00506 latency).
 I1216.73 Micro all activory. Models Lateron. Micro Address: Biolic and Sciences: Discrict: 77. (Austrek Computer) help scan report for 172.16.4.75 Micro Address: Biolic and Sciences: All All All All All All All All All Al	W 172164.78	<u>MML ADDITESSE</u> DDITOCIONFLACH.CH.ASUSCER LONDUCET) Mmap scan report for 172.16.4.74
Microsoft Microsoft <t< td=""><td>miern</td><td>Host is up (0.00408 latency).</td></t<>	miern	Host is up (0.00408 latency).
Mark server of a constant of a	TICI04.79	Nucl Address: B0:66:87:20c1E:77 (Asustek Computer)
Rest size up (0.00005 latence). Map scare sport for 12.1.6.4.7 Map scare sport for 12.1.6.4.7 Map scare sport for 12.1.6.4.7 Map scare sport for 12.1.6.4.7 Map scare sport for 12.1.6.4.8 Map scare sport for 12.1.6.4.9 Map scare sport for 112.1.6.4.8 Map scare sport for 112.1.6.4.8 Map scare sport for 112.1.6.4.8 Map scare sport for 112.1.6.4.8 Map scare scare (11 hosts up) scamed in 11.02 sconds Map scare scale (11 hosts up) scared in 11.02 sconds	W 17716430	More service of a factor of the service of the serv
Retists More is up (0.00305 latency). More scar report for 12.16.4.7 More scar report for 12.16.4.7 More scar report for 12.16.4.78 More scar report for 12.16.4.78 More scar report for 12.16.4.78 More scar report for 12.16.4.79 More scar report for 12.16.4.89 More scar report for 12.16.4.80 More scar report for 12.16.5.80 More scar report for 12.26.5.80 More scar report for 12.26.5		<u>MAK HAWATESSI</u> DEFICIENT (ASUSTER CUMPULET) Mag scan report for 172.16.4.76
Ref Address: Bords: Srial And Kaustek Lomputer) Map scan report for 172.16.4.77 Host is up (0.00095 latery). Will address: Block: SriaceALDB (Austek Computer) Map scan report for 172.16.4.79 Host is up (0.0005 latery). Will address: Block: SriaceALDB (Austek Computer) Host is up (0.0005 latery). Will address: Block: SriaceALDB (Austek Computer) Host is up (0.0005 latery). Will address: Block: SriaceALDB (Austek Computer) Host is up (0.0005 latery). Will address: Block: SriaceALDB (Austek Computer) Host is up (0.0005 latery). Will address: Block: SriaceALDB (Austek Computer) Host is up (0.0001 latery). Map come: IS IP addresses (11 hosts up) scanned in 11.00 seconds		Host is up (0.00308 latency).
Host is up (0.0036 latency). Muc Address: Bhoris:0F:25:25:00 (Asustek Computer) Muc Address: Bhoris:25:25:00 (Asustek Computer) Must is up (0.0026 latency). Muc Address: Bhoris:25:22:24:39 (Asustek Computer) Mus Scan report for 172:16.4.79 Mus Scan report for 172.16.4.89 Mus Scan report for 172.16.4.89 Mus Gadress: Bhoris:25:24:39 (Asustek Computer) Mus dadress: Bhoris:25:24:30 (Asustek Computer) Mus dadress: Bhoris:25:24:39 (Asustek Computer) Mus dadress: Bhoris:25:24:30 (Asustek Computer) Mus dadress: 25:24:30 (Asustek Computer) Mus dadress: 25:24:30 (Asustek Computer) Mus dadress: 25:24:30 (Asustek Co		<u>MK. Address.</u> B0:06:06:10:2.22/140 (Asustek Lomputer) Mman scan report for 172.16.4.77
Muc Address: B0:06:0F12.05.45:0D (Asustek Computer) Must scan report for 172.16.4.78 Host is up (0.00205 latency). Wuch Address: B0:06:0F12.05.4.79 Host is up (0.00205 latency). With scan report for 172.16.4.79 Host is up (0.00205 latency). With Address: B0:0F12.02.4199 (Asustek Computer) Must dome: 15 1P addresses (11 hosts up) scanned in 11.02 seconds Must dome: 15 1P addresses (11 hosts up) scanned in 11.02 seconds		Host is up (0.00306 latency).
Rink to sur report for 172.00.4.0 How to scan report for 172.16.4.79 Nump scan report for 172.16.4.79 How Address B0:66:0F:2C:20:44;90 Kat Address B0:66:0F:2C:24:49 Nump scan report for 172.16.4.90 Nump s		NMC Address: B0:66:66:66:66:06:00 (Asustek Computer)
Muc Address: B0:6E:0F:2C:0FA2 (Asustek Computer) Nump scan report for 112.16.4.79 Nump scan report for 112.16.4.30 Much Address: B0:6E:0F:2C:2F3+79 (Asustek Computer) Numb scan report for 112.16.4.80 Musp dome: 15 1P addresses (11 hosts up) scanned in 11.02 seconds Rite Hosts		hest scal reput for initiality of the second scale s
Nump scan report for 112.16.4.79 Huts tis up (0.00205 latency). Much address: 00:312.03.199 (Asustek Computer) Nump scan report for 112.4.80 Host is up (0.00205 latency). Num dddress: 00:43:CD:07-43:00 (Asustek Computer) Num ddnes: 15 IP addresses (11 hosts up) scanned in 11.02 seconds Fike Hosts		NMC_Address_ B0:66:86:20:28:42 (Asustek Computer)
Host is up (0.00206 latency). Map scan report for 121:2(2:4:9) (Asustek Computer) Map scan report for 121:2(2:4:9) (Asustek Computer) Map denes: 15 (0:0026 latency). Map dene: 15 (0:0016 sets (11 hosts up) scanned in 11.02 seconds Filer Hosts		Map scan report for 172.16.4.79
Ret Host		these starts (b) (000000) addressing to the start of the
Host is up (0.00206 latency). NML Addresses 60-45:CB:07-45:00 (Austek Computer) NMLD done: 15 IP addresses (11 hosts up) scanned in 11.02 seconds Fiket Hosts		hand. Factor is relative for the factor is relat
MMC Addresss 60-45:CB:07-45:08 (Asustek Computer) Mwap dome: 15 IP addresses (11 hosts up) scanned in 11.02 seconds Fiket Hosts		Host is up (0.00206 latency).
File Host		<u>NMC Address:</u> 60:45:(26:87:45:08 (Asustek Computer) Weam Adment 17 TP addresses (11 hosts wull stranded in 11 00 serveds
Liker Hosts		
First Hosts		
	Filter Hosts	

Service:

1	Port 1	Durbert 4			
0		PICEOCOL 1	State (Service	Version
1.	135	tcp	open	msrpc	Microsoft Windows RPC
0	139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
0	445	tcp	open	microsoft-d	s Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
0	49152	tcp	open	msrpc	Microsoft Windows RPC
0	49153	tcp	open	msrpc	Microsoft Windows RPC
0	49154	tcp	open	msipc	Microsoft Windows RPC
0	49167	tcp	open	msrpc	Microsoft Windows RPC

Topology:

Nmap Output	Ports / Hosts	Topology	Host Details	Scans	
Hosts Viewer	Fisheye Con	trols			



Result:

The above program has been executed successfully and the output is verified.

Aim:

To use burp proxy to capture and modify the message.

Algorithm:

Step1: start the process.

Step2: Open the Burp proxy tool.

Step3: First, ensure that Burp is correctly configured with your browser. In the Burp Proxy "Intercept" tab ensure "Intercept is off".

Step4: To visit the web application you are testing in your browser.

Access the log in page of the web application.

Step5: Return to Burp. In the Proxy Intercept tab, ensure "Intercept is on".

Step6: Enter login details in to the login form and submit the request. by clicking "Login".

Step7: Return to Burp. The raw request details should now be displayed In the Proxy "Intercept" tab. Right click on the request to bring up the context menu and click "Do an active scan."

Step8: The results of the scan are displayed in the Target "Site map" tab. The Scanner has detected that the application has an issue; "Clear text submission of password".

- Step9: By clicking on an individual issue we can view a description of the vulnerability and suggested remediation in the "Advisory tab". The full request and response are also shown.
- Step10: Burp Scanner checks for a variety of types of data exposure, SSH keys, credit card numbers and email addresses, etc.

Step1:

Targe	t Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Deco
Interc	ept HTT	P history	WebSoc	kets history	/ Options		
Forward							
Fc	orward		Drop	Interc	ept is off	Actio	n

Step2:

Isername		
osername.		
Password:		

Step3:

Targe	et Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Deco
Intere	cept HT	FP history	WebSoc	kets history	Options		
Fc	orward		Drop	Interce	pt is on	Action	
Daves	Darame	Headore	Hay				

Step4

lsername:	
test	
assword:	

Step5:

Target Proxy Spider Scan	ner Intruder	Repeater	Sequencer	Deco
Intercept HTTP history Web	Sockets history	Options		
Request to http://172.16.67	7.136:80			
Forward Drop	Interce	pt is on	Action	1
Raw Params Headers Hex				
POST /wordpress/wp-login.p Host: 172.16.67.136	hp HTTP/1.1			
User-Agent: Mozilla/5.0 (i	Phone; CPU iP	Phone OS	5 1 1 ike 1	fac OS
Accept: text/html,applica Accept_Language: en_GB_en	Send to Spide	er		g=0.9,
Accept-Encoding: gzip, de	Do an active	scan	1	
Referer: http://172.16.67	Send to Intru	der	% +I	
Cookie: acopendivids=swin	Send to Repe	ater	3€+R	upswi
Content-Type: application	Send to Sequ	encer		

Step6:



Step7:

Path:



/wordpress/

Step8:

Issues	
Oleartext submission of password [2]	
Heassword field with autocomplete enabled [2]	
i Cross-domain Referer leakage	
i Cookie without HttpOnly flag set	
i File upload functionality	
i Email addresses disclosed	
i Multiple content types specified	
i Frameable response (potential Clickjacking) [6]	
Advisory Request Response	
1 Email addresses disclosed	

Confidence: Certain

Result:

The above program has been executed successfully and output is verified.

Aim:

To demonstrate sending of protected word document.

Algorithm:

- Step 1: Open the new Microsoft word document.
- Step 2: click the office button \rightarrow save as \rightarrow word document \rightarrow

Tools \rightarrow general options.

Step 3: In general options \rightarrow type password to open and modify a

Document and re-enter the password to open and modify the document.

- Step 4: save the document and close the file.
- Step 5: The protected word document is attached to mail-id.
- Step 6: In separate mail send the password without mentioning the

Subject.

Step 7: Stop the process.

Step1:



Step2:

1 Book1 IS 2 Book2 3 Book3 4 Book1.xls 5 Book1 5 Book1 5 Book1 5 Book1 6 Book1.xls 7 2 6 Book1 7 2 8 network1 9 New Microsoft Office Excel Worksheet Iris Iris	
Qpen 2 Book2 3 Book3 4 4 Book1.xls 5 5 Book1 6 5 Book1 5 5 Book1 5 6 Book1 IS 6 6 Rook1 IS 6 9 Print 2 New Microsoft Office Excel Worksheet 1ris Iris Iris Iris	-[=1
2 Book3 4 Book1.xls 5 Book1 5 Book1	-0=1
Save 4 Book1.xls 5 Book1 6 Book1.xls 7 Book1 8 Book1 9 New Microsoft Office Excel Worksheet 1ris Iris	-1:1
Save 5 Book1 Save As 6 Book1.xls Z Book1 IS 8 network1 Print 9 New Microsoft Office Excel Worksheet Iris Iris	-6=1
Save As Save As Print Print Save As Save As	-6=1
Save As Z Book1 IS Print 9 New Microsoft Office Excel Worksheet Iris Iris	-[;=1
Print [§] network1 9 New Microsoft Office Excel Worksheet Iris	-[i=1
Print 9 New Microsoft Office Excel Worksheet Iris	-6=1
Iris	-6-0
	-[ai
Prepare iris	-0-4
k	-6=1
Sen <u>d</u> > vote	-6=1
vote3	-[;=1
🥐 P <u>u</u> blish 🕨 vote	-()=1
is.xls	-6=0
Close 9	-(=1

Step3:



Step4:

Organize + Ne	nv folde				1111 - 16
Desktop Downloads Downloads Decent Placer Documents Music Picturec Videos		Name IS Lab kathi New folder New folder New Microsoft Office W New Microsoft Word Do Sample Weke Data Sets	ord Document cument (2) is lab	Date modified 9/3/2018 1:30 PM 8/23/2018 9:34 AM 8/1/2018 9:50 AM 9/3/2018 1:31 PM 8/27/2018 2:31 PM 8/22/2018 9:14 AM	Type File folder File folder Microsoft Office Microsoft Office
Computer		4 (I			
File name	Inform	nation Security Book1			
Save as type:	Word	Decument			
Authorsi	A. 810 million				

Step5:



Step6:

Reenter password to open:		
Caution: If you lose or forg recovered. (Remember tha	et the passwo t passwords a	rd, it cannot be re case sensitive
	ОК	Cancel

Step7:



Result: The above program has been executed successfully and the output is verified.

Aim:

To demonstrate sending or a digitally signed document.

Algorithm:

Step 1: Open a word document.

- Step 2: Type a content in word document with letter format.
- Step 3: place the curser to insert the digitally signed signature.
- Step 4: Click insert menu →signature line→signature set up dialog Box type the suggested signer, etc.
- Step 5: The signature line is created in the word document and right click \rightarrow select sign option \rightarrow select image.
- Step 6: Finally the digitally signed document is created with date

line

Leave Letter

From

уууууууу,

III B.SC (cs),

Department of computer science,

Karpagam Academy of Heigher Education,

Eachanari,

Coimbatore-641021.

То

The Head of the department, Department of computer science, Karpagam Academy of Heigher Education, Eachanari, Coimbatore-641021.

Respected Madam,

I am suffering from fever. I am unable to attend the class So, leave for grant me two days with your permission (03/09/2018 to 04/09/2018).

Thanking You,

Your's faithfully,

9/10/2018

lhon уууууууу

Result:

The above program has been executed successfully. And output is verified.

Aim:

To demonstrate sending of a protected worksheet.

Algorithm:

- Step 1: Open the excel worksheet.
- Step 2: click the office button \rightarrow prepare \rightarrow Encryption document.
- Step 3: enter the password and re-enter the password in encryption Document.
- Step 4: Enter the data in worksheet and close the file.
- Step 5: The protected excel document is attached to mail-id.
- Step 6: In separate mail send the password without mentioning the Subject.

Step 7: Stop the process.

Step1:

0	1	19									dinit.	Menter	tine									G	
18		FREE.	10	iét.	Pagetagoa	r Persola	Tata	Re/mi	Mexi Cheir													W -	$\sim \times$
1	1	a Cat	ę., .		Calles .	+ 11 + A	A' =		- Swa	Tert	Germa		4	h		-	Ter P	-	Σ Aptoins T Aptoins	1	Æ		
-		than	rat Pai	ette	month of	I III I I WAR		2 2 X	at annu	CE CHIORY		MON GOM	4802	Plenattro	* ei Tator *	Mylet.*	aner beer	-	(20m*	film.+	Select+		
_	194	19381			1	/int	15		Farmers .			turder.			2019/011		Criti		-	tuming			1000
		198		•	5 B																		1
2	A.	З.,	C.	D	ε	ŧ:	6	1.1	1.1	35	1 K.	、法		М.	N.	.0.	P.S	Q	В	5	:7	U.	
1					Serial No.	stud name	stud_id	class	Course_pgm	dept	marki	mark2	tot	al mari	avg								- 11
2						Arauth	05U301	3rd year	1.Sc	CS		15 J	76	141	36.5								
3					3	2 Bala	154102	3rd year	B.Sc	ĊŚ	1.1	94 3	52	100	53								
4						1 Chithra	664103	3rd year	B.Sc	CS		34 3	14	38	19								
5						1 Divya	CSU104	3rd year	B.Sc	C5		15 4	48	63	31.5								
-10					- 3	5 Ezhil	ctu105	3rd year	B.Sc	CS		12 9	68	155	77.5								
7						6 Fathima	csu106	3rd year	B.5z	CS		53 3	53	105	55		-	_					
#						7 Gayathei	csu107	3rd year	B/Sc	CS	1.2	19 1	14	93	46.5								
9					3	E Hari	66¢usta	3rd year	B.Sc	CS .		18 4	43	70	35		1						
30					3	9 Indhu	FSU109	3rd year	8.5c	CS	. 4	14 t	53	140	73								
11					1	Lianani	csu110	Brd year	8.5c	CS	1	11 4	43	64	32								
33					1	Karthick	094111	3rd year	8.5c	CS.		54 J	35		49.5								
33					1	2 Lavanya	csu112	3rd year	B.Sc	CS	1	1 8	54	113	56.5								
34					1	1 Mani	ctul13	Brd year	B.Sc	CS		18 1	15	103	51.5								
35						I Naveen	csu114	3rd year	8.5c	CS	1.1	n 1	65	137	663								
26					1	S Oshma	ctul15	3rd year	B.Sc	ES		53 1	78	131	65.5								
17					3	5 Prayven	tsut16	Std year	R.52	cs		54]	18	52	45								
38					1	7 Queen	CSU117	3rd year	B.Sc	CS		13 1	17	114	57								
19					5	i Raj	csul18	3rd year	B.Sc	ES .		46 3	16	62	33								
30					1	I Satheesh	094119	3rd year	8.5c	CS		ц. з	14	135	67.5								
21					2	7 Thereni	csu120	3rd year	8.5c	CS	1	21 4	42	63	33.5								
22					2	1:Usha	csu121	3rd year	B.Sc	CS		22 6	66	- 88	44								
23					2	2 Varsha	C5U122	3rd year	B.Sc	05	. 1	52 4	15	101	50.5								
24					2	Tiavan .	ctu123	3rd year	B.Sc	CS		28 3	71	99	49.5								
25								1					1		-							-	
Beach		504	all.	278	12 576903	a de										_				Acri col a	100 (C)	T.	The second

Step2:



Step3:



Step4:

ncrypt the contents of	f this file
Passwo <u>r</u> d:	
Caution: If you lose or recovered. It is advisal their corresponding do	forget the password, it cannot be ble to keep a list of passwords and cument names in a safe place.

Step5:



Result:

The above program has been executed successfully and the output s verified.

Aim:

To demonstrate use of stenography tool.

Algorithm:

- Step 1: Start \rightarrow Xiao Steganography 2.6.1 \rightarrow add file \rightarrow load target file.
- Step 2: The image is loaded in the target file.
- Step 3: create a worksheet and save the file with .xls extension.
- Step 4: click next option button \rightarrow add file \rightarrow browse the worksheet.
- Step 5: click next option button \rightarrow choose encryption and hashing

Algorithms and type password in given textbox.

Step 6: click next option button \rightarrow save the file \rightarrow save as type \rightarrow bmp File type \rightarrow save \rightarrow finish.

Step 7: click target file \rightarrow select source file \rightarrow next option button \rightarrow

Enter the password to unlock the file.

Step 8: click the extract file option button and save the file with

.xls extension \rightarrow save.

Step 9: we get, file extract was successful! Message.

Step 10: Open the source file in worksheet.

Step1:



Step2:



Step3:

👩 Add file to ima	Add file to image		
Step 2: Sele	ct the file must be add	l into the target file:	:
Remaining KB	: 83.425		
File Type	Name	Size (KB)	
xls	Book3	16.500	
In Add File	Remove File		
E Back	Next C Finish		

Step4:

ep 3: Encryptation Options		
Encryption Algorithms © RC2 C RC4 C DES C Triple DES C Triple DES 112	Hashing Algo	C MD4
issword: ****		

Step5:



Step6:

Step7:



Step8:



Step9:

Xiao 2.6.1	×
File extract	was successful!
	ОК

Result:

The above program has been executed successfully and the output is verified.

GPG Utility

Date:

Aim:

To demonstrate use of GPG utility for singing and encrypting purposes.

Algorithm:

Step1: start the process.

Step2: Open the GPG command line tool

Step3: Open Git Bash.

Step4: Generate a GPG key pair. Since there are multiple versions of GPG,to

Needed a consult the relevant *man page* to find the appropriate key generation command.

Step5: Paste the text below to generate a GPG key pair.

Step6: The gpg --full-generate-key command doesn't work. Paste the text below

Step7:At the prompt, specify the kind of key we want, or press Enter to accept

The default RSA and RSA Algorithm.

Step8:Enter the desired key size. The maximum key size of 4096.

Step9:Enter the length of time the key should be valid. Press Enter to specify

The default selection, indicating that the key doesn't expire.

Step10:Verify that your selections are correct.Enter your user ID information.

Type a secure passphrase.

Step11:Use the gpg --list-secret-keys --keyid-format LONG command to list GPG keys for which you have both a public and private key. A private key is required for signing commits or tags.

Step12:From the list of GPG keys, copy the GPG key ID to use. the GPG key ID is 3AA5C34371567BD2: Step13:Paste the text below, substituting in the GPG key ID to use.

the GPG key ID is 3AA5C34371567BD2:

- Step14:If we have multiple keys or are attempting to sign commits or tags with a key that doesn't match your committer identity the signing key.
- Step15:When committing changes in our local branch, add the -S flag to the git commit command:
- Step16:If we're using GPG, after we create our commit, provide the passphrase you set up when you generated your GPG key.

Step17:When we've finished creating commits locally, push them to our

remote repository on GitHub:

Step18:On GitHub, navigate to our pull request.

Step19:On the pull request, click Commits.

Step20:To view more detailed information about the verified signature, click Verified.

o gpg --full-generate-key o gpg --default-new-key-algo rsa4096 --gen-key 2. gpg --list-secret-keys --keyid-format LONG 3. gpg --list-secret-keys --keyid-format LONG 4. /Users/hubot/.gnupg/secring.gpg 5. -------6. sec 4096R/3AA5C34371567BD2 2016-03-10 [expires: 2017-03-10] 7. uid Hubot 8. ssb 4096R/42B317FD4BA89E7A 2016-03-10 9. gpg --armor --export 3AA5C34371567BD2 10. # Prints the GPG key ID, in ASCII armor format 11. git commit -S -m your commit message 12. # Creates a signed commit 13. git push 14. # Pushes your local commits to the remote repository

Conversation 38

-O- Commits 6

E) Files changed 1

Result:

The above program has been executed successfully and the output is verified.