CYBER SECURITY FUNDAMENTALS AND LAW LAB MANUAL

Prepared by

Dr Shreema Shetty

Associate professor

Department of CSE

Sahyadri college of Engineering and Management

Experiment List

1. Demonstrate Network packet analysis using WireShark tool.

2. Demonstrate Web penetration testing using BURP Suite tool.

3. Show Network mapping and port scanning using Nmap tool.

4. Implement a code to simulate buffer overflow attack.

5. Demonstrate of Cryptographic algorithm using JCryp tool.

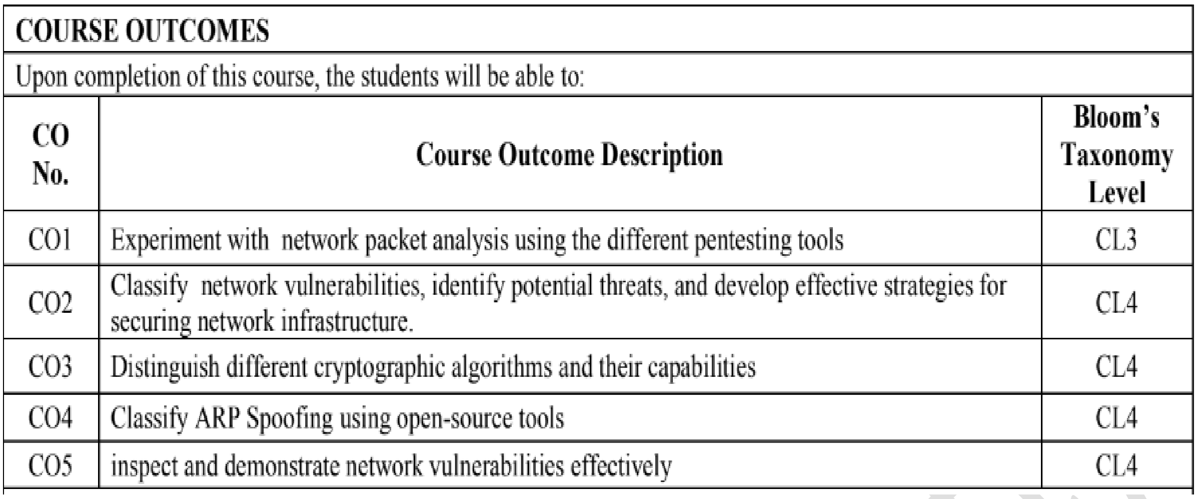
6. Demonstrate Network reconnaissance using WHOIS tool.

7. Show how to detect ARP Spoofing using open-source tool ARPWATCH.

8. Demonstrate network vulnerabilities by scanning network using Nessus tool.

9. Demonstrate network testbed Emulab.

10. Study of Information Technology Act, 2000 (India)



COURSE OUTCOMES		
Upon completion of this course, the students will be able to:		
CO No.	**Course Outcome Description**	**Bloom's Taxonomy Level**
CO1	Experiment with network packet analysis using the different pentesting tools	CL3
CO2	Classify network vulnerabilities, identify potential threats, and develop effective strategies for securing network infrastructure.	CL4
CO3	Distinguish different cryptographic algorithms and their capabilities	CL4
CO4	Classify ARP Spoofing using open-source tools	CL4
CO5	inspect and demonstrate network vulnerabilities effectively	CL4

Experiment 1: Demonstrate Network packet analysis using WireShark tool.

1. Aim: Study of packet sniffer tool Wireshark

2. Objectives: Identify different packets moving in/out of network using packet sniffer for network analysis.

3. Hardware / Software Required: Wireshark.

4. Theory:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets.

Applications:

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals beside these examples can be helpful in many other situations too.

As soon as you click the interface‘s name, you‘ll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system. If you‘re capturing on a wireless interface and have promiscuous mode enabled in your capture options, you‘ll also see other the other packets on the network. Wireshark uses colours to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.

Capturing Packets: After downloading and installing wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by clicking Capture Options.

5. Methodology:

To analyse network protocol packets follow steps given below:

1. Generate network traffic using browser.
2. Open wireshark.
3. Capture network data .
4. Use display filter to segregate network protocol packets.
5. Get required information corresponding different protocol such as Http,DNS, TCP and IP.

To get Machine details open window command prompt and type >> Ipconfig/all.

To get Website details open window command prompt and type >> ping (for example: www.sahyadri.edu.in)

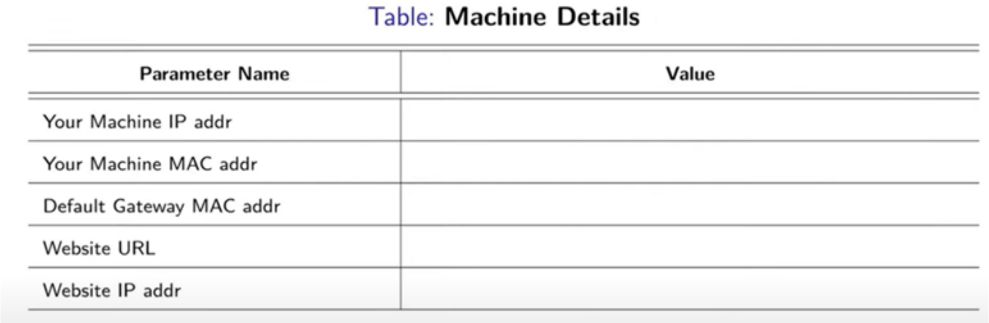


Table: **Machine Details**

Parameter Name	Value
Your Machine IP addr	
Your Machine MAC addr	
Default Gateway MAC addr	
Website URL	
Website IP addr	

HTTP and TCP Packet header:

To analyze HTTP packet type http in display filter of wireshark. For selected http packet the details regarding packet selected appears in third window gride.

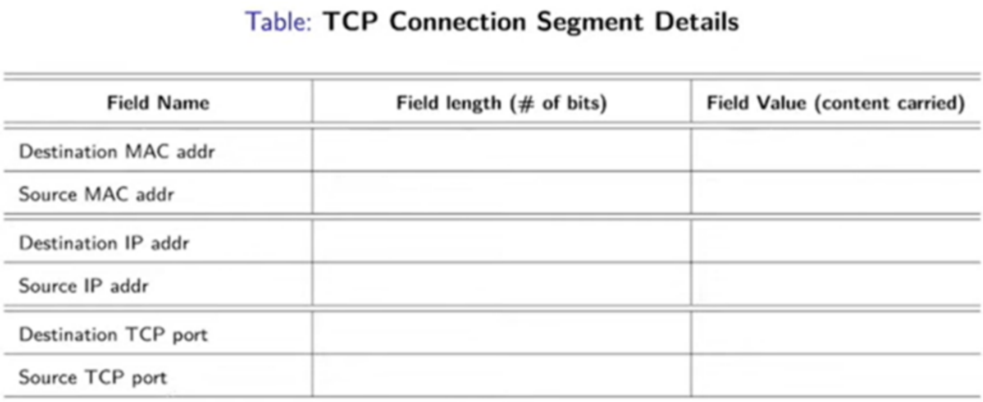


Table: TCP Connection Segment Details

Field Name	Field length (# of bits)	Field Value (content carried)
Destination MAC addr		
Source MAC addr		
Destination IP addr		
Source IP addr		
Destination TCP port		
Source TCP port		

Domain Name Server :

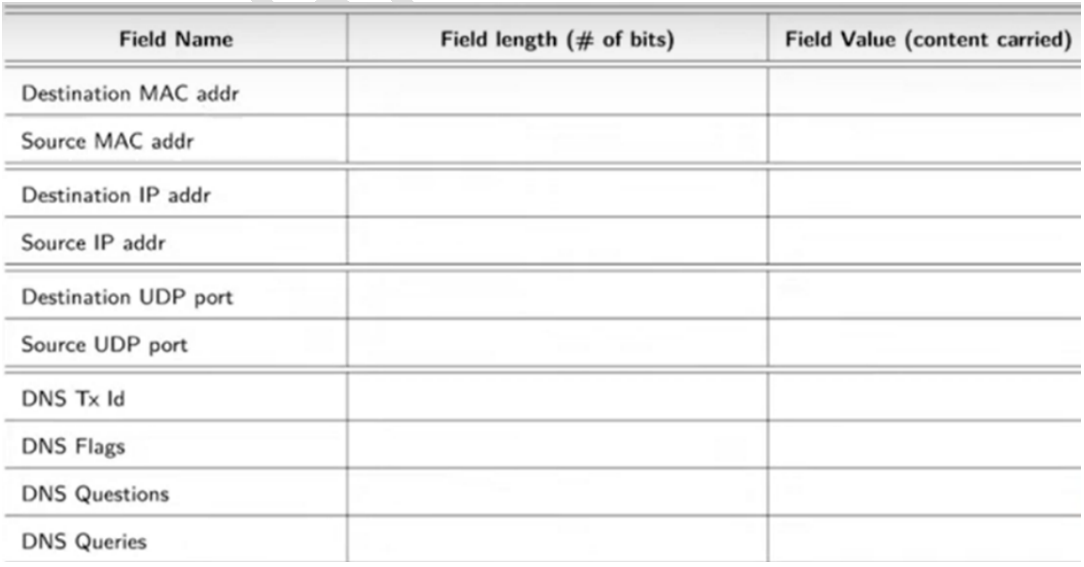
To analyze DNS packet , type “dns” in display filter of wireshark. For selected dns packet the details regarding packet selected appears in third window gride.

Window cmd prompt command:

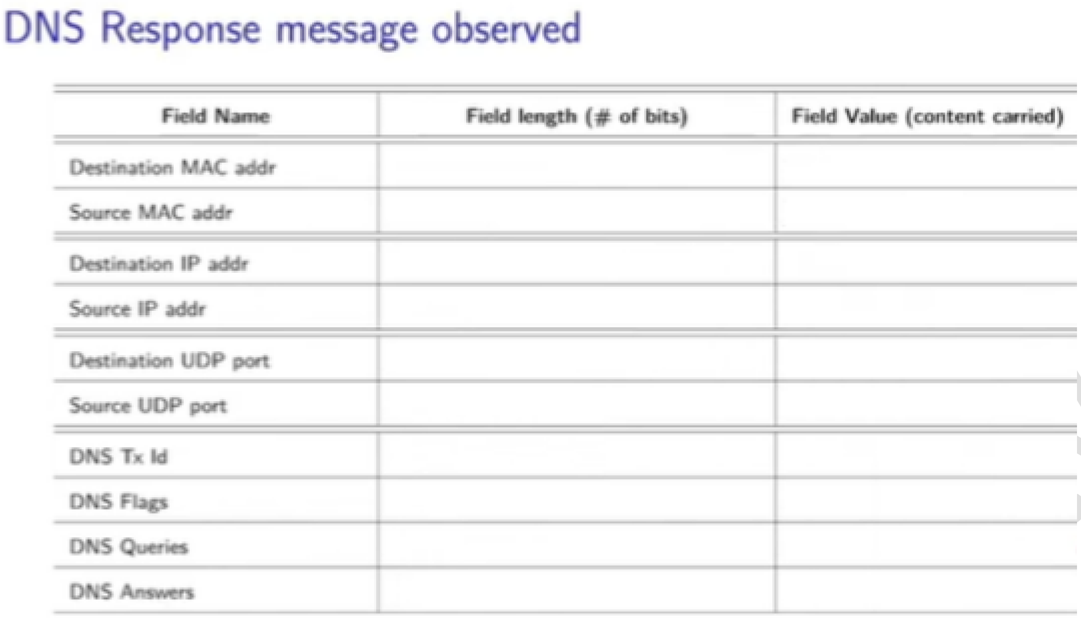
- Ipconfig / flushdns (clear)
- Ipconfig /displaydns
- ping (for example: www.sahyadri.edu.in)

We can see that DNS query generated and response coming to our machine .

DNS Query message observed:



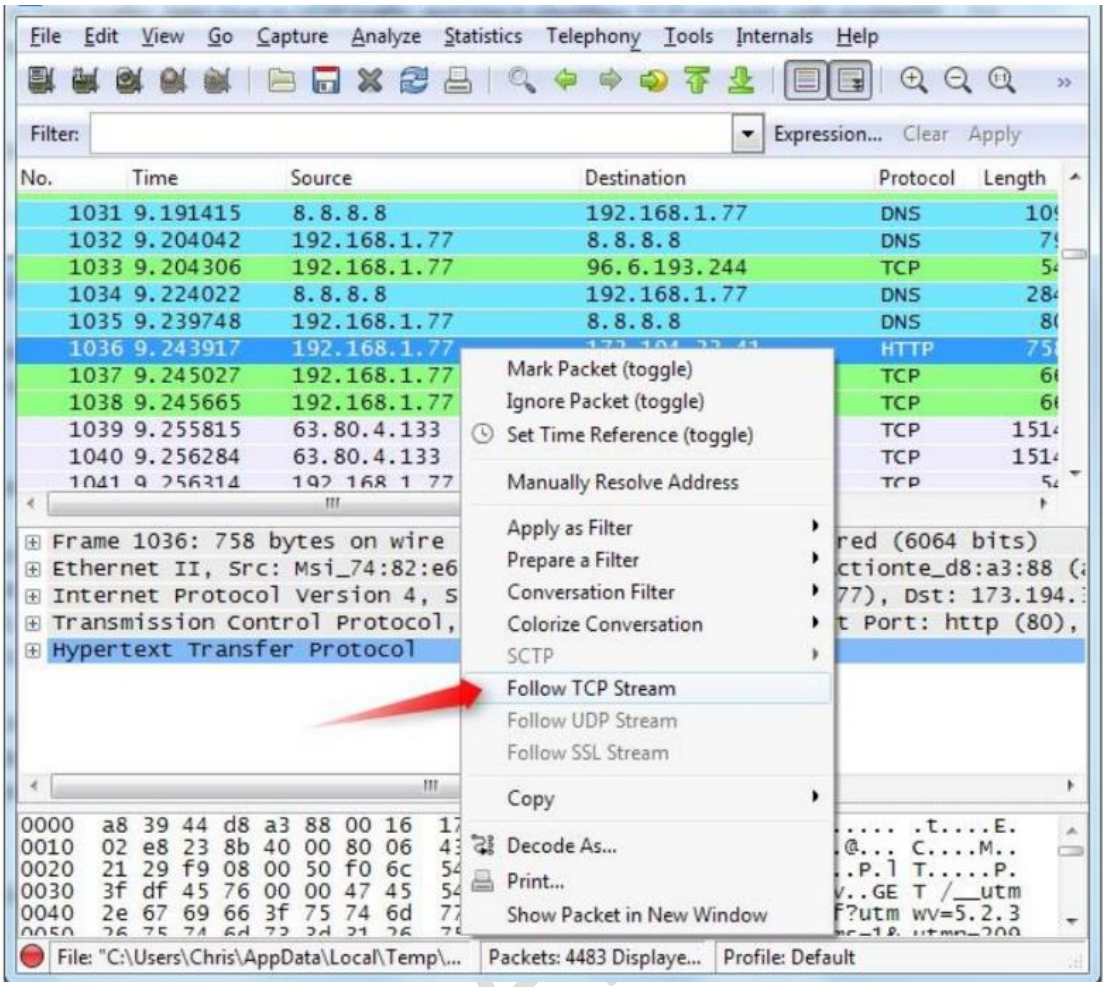
Field Name	Field length (# of bits)	Field Value (content carried)
Destination MAC addr		
Source MAC addr		
Destination IP addr		
Source IP addr		
Destination UDP port		
Source UDP port		
DNS Tx Id		
DNS Flags		
DNS Questions		
DNS Queries		



DNS Response message observed

Field Name	Field length (# of bits)	Field Value (content carried)
Destination MAC addr		
Source MAC addr		
Destination IP addr		
Source IP addr		
Destination UDP port		
Source UDP port		
DNS Tx Id		
DNS Flags		
DNS Queries		
DNS Answers		

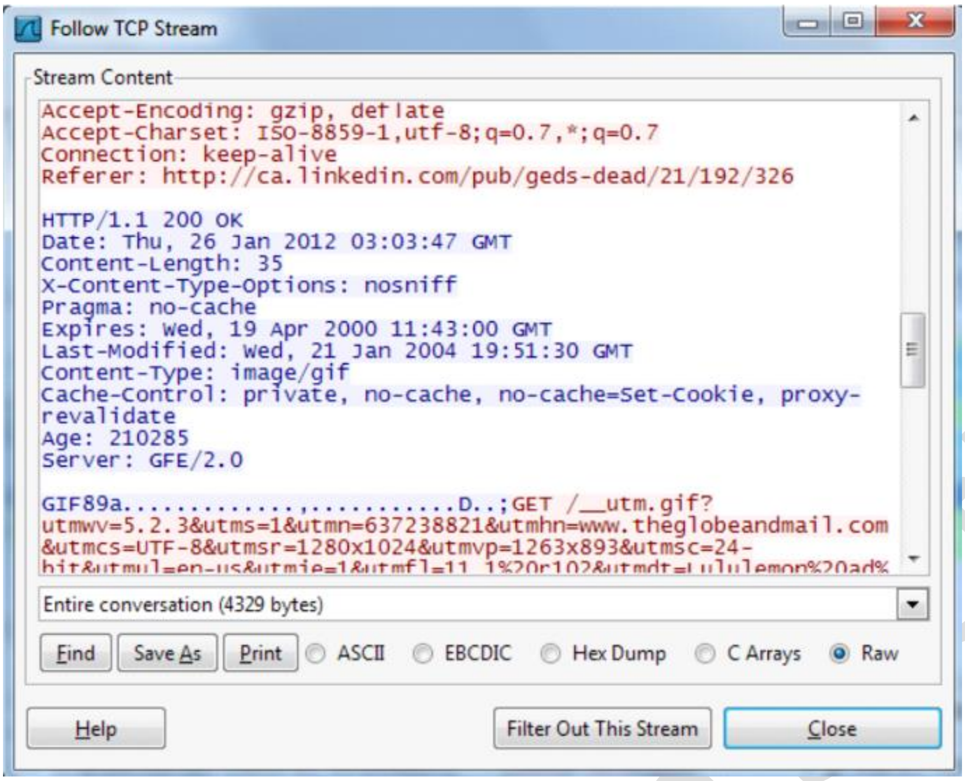
You‘ll see the full conversation between the client and the server.


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length
1031	9.191415	8.8.8.8	192.168.1.77	DNS	10
1032	9.204042	192.168.1.77	8.8.8.8	DNS	7
1033	9.204306	192.168.1.77	96.6.193.244	TCP	5
1034	9.224022	8.8.8.8	192.168.1.77	DNS	28
1035	9.239748	192.168.1.77	8.8.8.8	DNS	8
1036	9.243917	192.168.1.77	173.194.33.41	HTTP	75
1037	9.245027	192.168.1.77		TCP	6
1038	9.245665	192.168.1.77		TCP	6
1039	9.255815	63.80.4.133		TCP	151
1040	9.256284	63.80.4.133		TCP	151
1041	9.256314	192.168.1.77		TCP	5

```
⊞ Frame 1036: 758 bytes on wire              red (6064 bits)
⊞ Ethernet II, Src: Msi_74:82:e6             ctionte_d8:a3:88 (
⊞ Internet Protocol Version 4, S             77), Dst: 173.194.
⊞ Transmission Control Protocol,             t Port: http (80),
⊞ Hypertext Transfer Protocol
```

```
0000  a8 39 44 d8 a3 88 00 16 17       ..... .t....E.
0010  02 e8 23 8b 40 00 80 06 43       .@... C....M..
0020  21 29 f9 08 00 50 f0 6c 54       ..P.l T.....P.
0030  3f df 45 76 00 00 47 45 54       V..GE T /__utm
0040  2e 67 69 66 3f 75 74 6d 77       f?utm wv=5.2.3
```



```
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: keep-alive
Referer: http://ca.linkedin.com/pub/geds-dead/21/192/326

HTTP/1.1 200 OK
Date: Thu, 26 Jan 2012 03:03:47 GMT
Content-Length: 35
X-Content-Type-Options: nosniff
Pragma: no-cache
Expires: Wed, 19 Apr 2000 11:43:00 GMT
Last-Modified: Wed, 21 Jan 2004 19:51:30 GMT
Content-Type: image/gif
Cache-Control: private, no-cache, no-cache=Set-Cookie, proxy-
revalidate
Age: 210285
Server: GFE/2.0

GIF89a.............,...........D..;GET /__utm.gif?
utmwv=5.2.3&utms=1&utmn=637238821&utmhn=www.theglobeandmail.com
&utmcs=UTF-8&utmsr=1280x1024&utmvp=1263x893&utmsc=24-
hit&utmul=en-us&utmje=1&utmfl=11.1%20r102&utmdt=Lululemon%20ad%
```

Entire conversation (4329 bytes)

Close the window and you‘ll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation.

6. Conclusion:

In this experiment we analyze packet sniffing tool that monitor network traffic transmitted between legitimate users or in the network. The packet sniffer is network monitoring tool. It is opted for network monitoring, traffic analysis, troubleshooting, Packet grapping, message, protocol analysis, penetration testing and many other purposes.

Experiment 2: Demonstrate Web penetration testing using BURP Suite tool.

1. Aim: The aim is to provide a foundation in performing security testing of web applications using Burp Suite.

2. Objectives: Understand Burp Suite and its tools for web application testing process.

3. Hardware / Software Required: BURP suite tool

4. Theory:

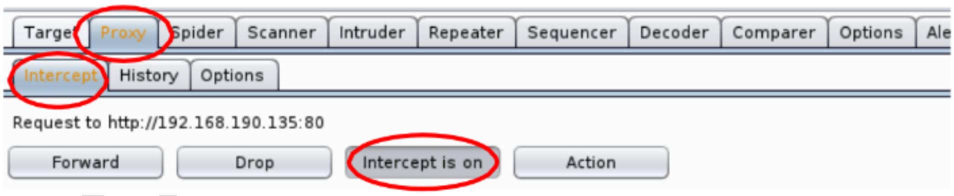
Burp Suite created by PortSwigger Web Security is a Java-based integrated software platform of tools for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. This includes key components such as: Proxy, Spider, Scanner, Intruder, Repeater and Sequencer.

5. Methodology:

- **Intercepting Proxy**

In Burp Suite, intercepting Proxy lets you inspect and modify traffic between your browser and the target application. Therefore, by using Proxy tab in Burp Suite, we can intercept the communications between a client (such as a Web browser) and the server. For this, set up your browser to use a Proxy (127.0.0.1 on port 8080). (Hint: use: Edit > Preferences> Advanced > Network > Settings).

Go to Burp Suite and in the Proxy tab, set Intercept to on.



Request to http://192.168.190.135:80

Figure 1: BURP suite proxy tab.

Navigate to the **http://tutorialsninja** (demo web page) home page. Then switch to Burp Suite. Burp Suite proxy should intercept the request. Click **forward**. Now, go to your browser and check if you can see the homepage of tutorialsninja. Now, on the tutorialsninja homepage, click on **Login/Register** and go back to Intercept tab on Burp Suite. Right click and select **Send to Intruder** (Figure 2)

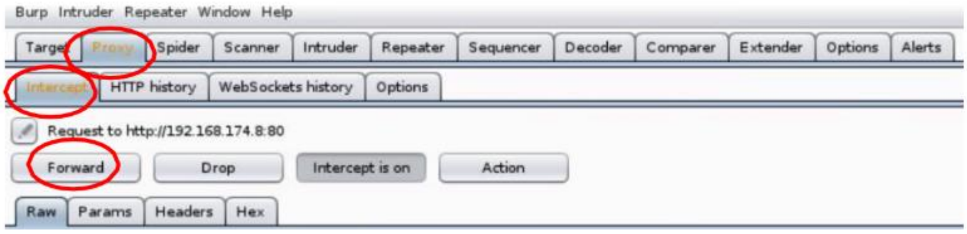
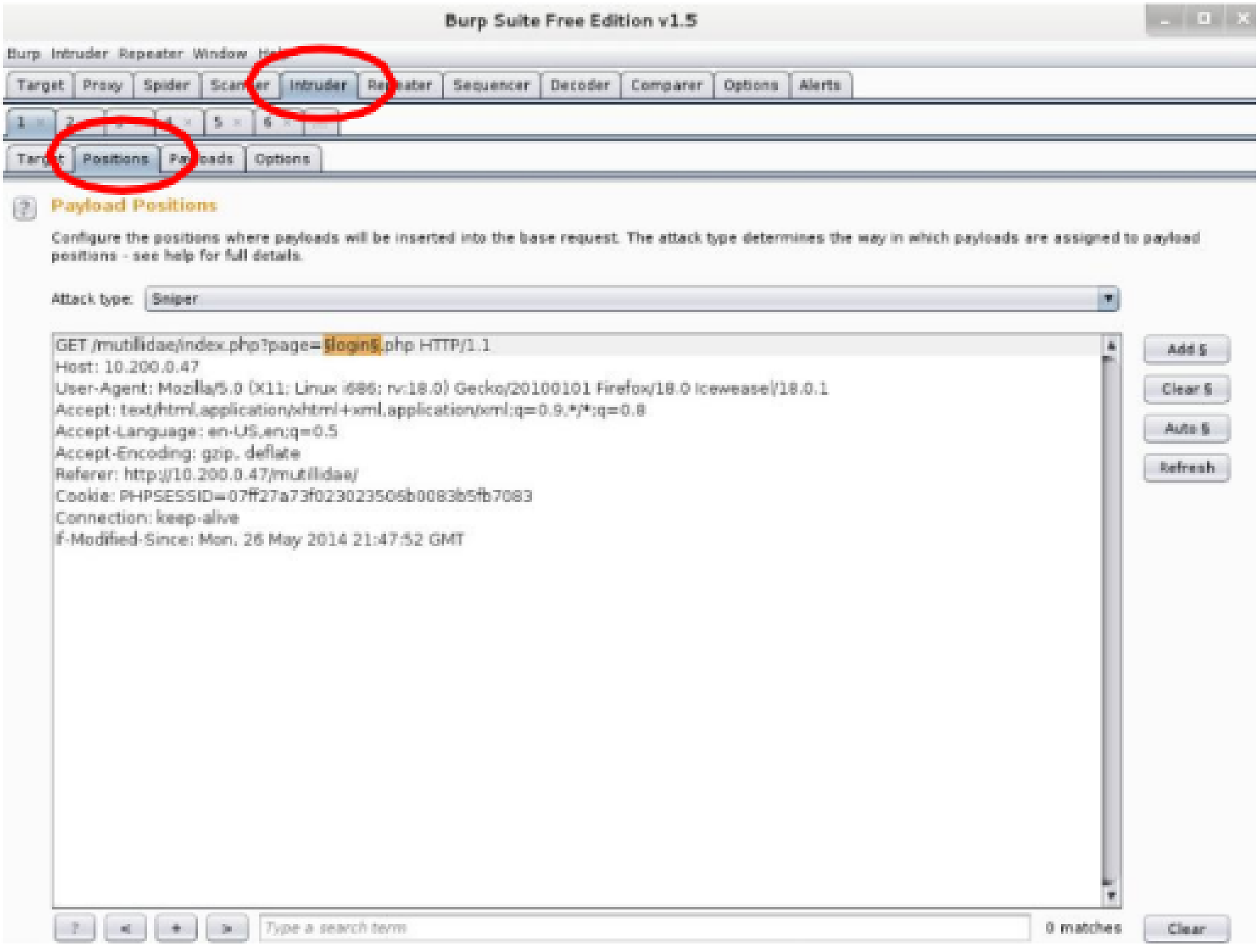


Figure 2: BURP suite proxy tab and forward tab.

Now, go to **intruder tab** and check if you can see the **login page** (Figure 3). Next identify the word/parameters that we are going to change (login). Clear $$ from Cookie but keep them for login ($login$).



Payload Positions

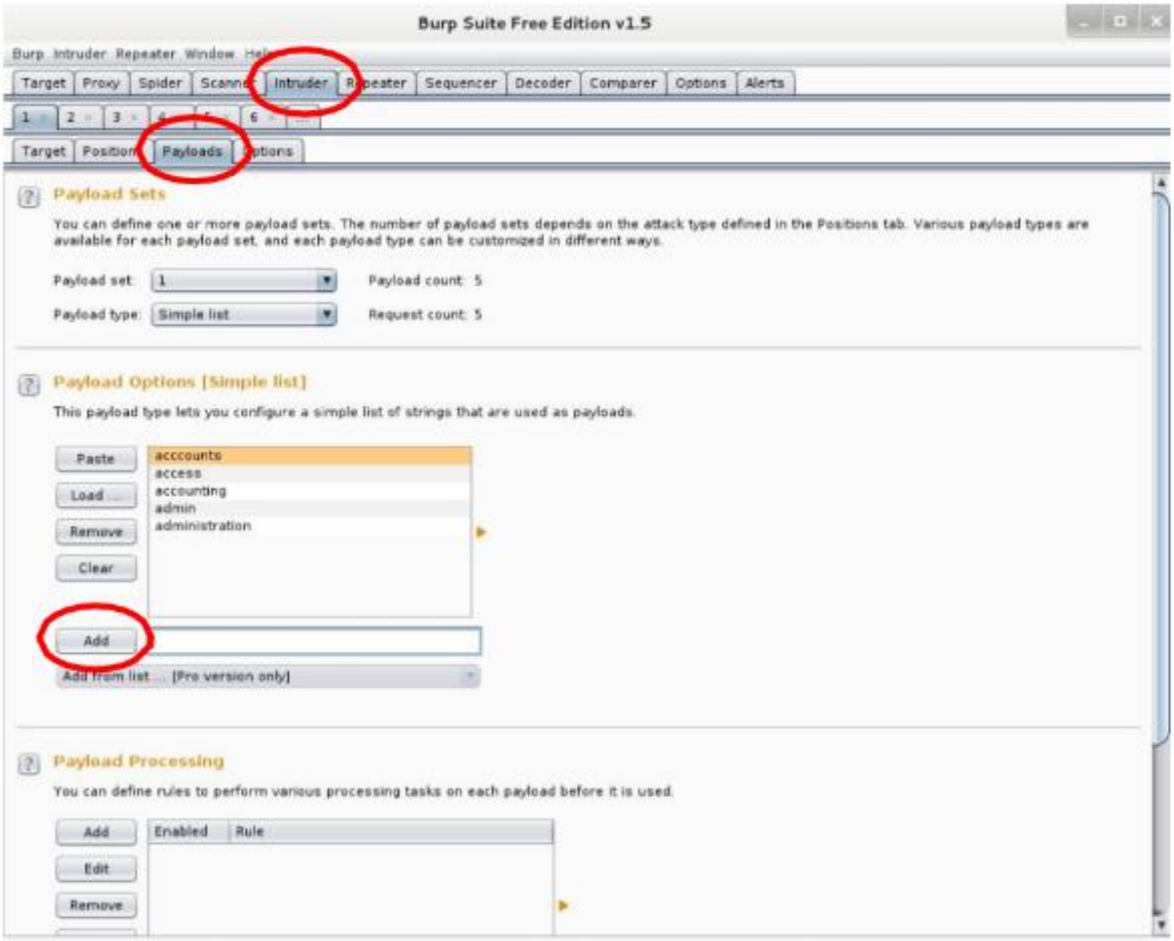
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
GET /mutillidae/index.php?page=$login$.php HTTP/1.1
Host: 10.200.0.47
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.200.0.47/mutillidae/
Cookie: PHPSESSID=07ff27a73f023023506b0083b5fb7083
Connection: keep-alive
If-Modified-Since: Mon, 26 May 2014 21:47:52 GMT
```

Figure 3: Intruder tab for logging page.

Select payloads tab (hint: payloads tab is next to the positions tab) (Figure 4). Go to the **Intruder>Payloads** tab and add some payload words to the list. Hint: type them one by one in the box below and then **press Add** (Figure 4).


Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
1 2 3 4 5 6 ...
Target Positions Payloads Options
Paste
Load ...
Remove
Clear
Add
Add from list ... [Pro version only]
Add
Edit
Remove
Enabled
Rule

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 5

Payload type: Simple list Request count: 5

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

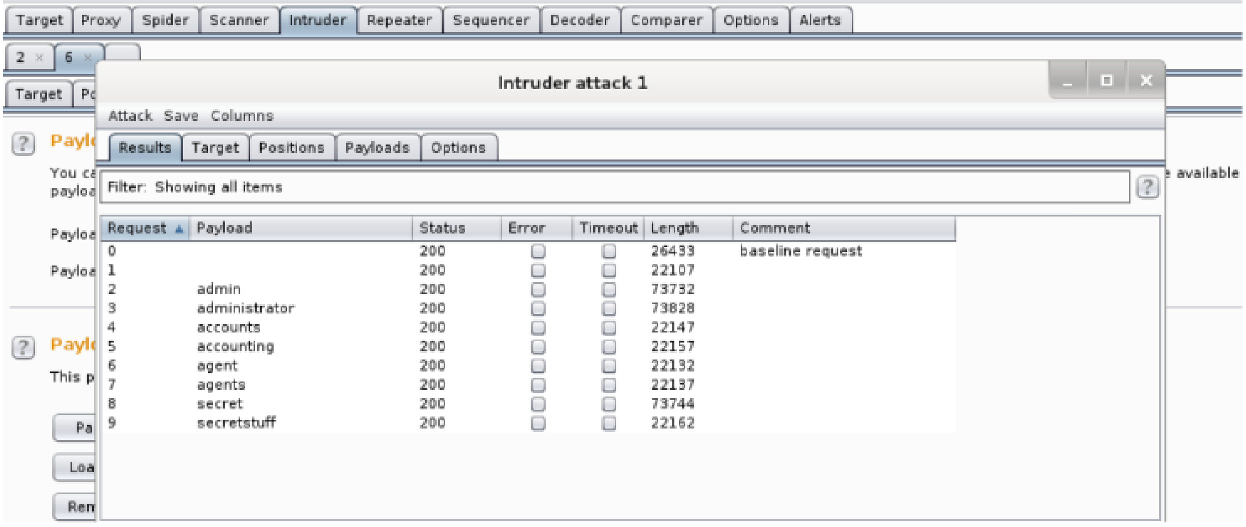
acccounts
access
accounting
admin
administration

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Figure 4: Adding payload list.

Run the brute-force fuzzer from the **Intruder>Start** Attack menu on top. The Fuzzing Attack window should be displayed and shows the progress (Figure 5). The **Request>Raw** tab , the Results show the Requests which are sent. Next the **Response>Raw** Tab shows what was returned from the web application for each response. The **Response>Render** shows the rendered page as a browser would display it.



Request ▲	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	26433	baseline request
1		200	☐	☐	22107	
2	admin	200	☐	☐	73732	
3	administrator	200	☐	☐	73828	
4	accounts	200	☐	☐	22147	
5	accounting	200	☐	☐	22157	
6	agent	200	☐	☐	22132	
7	agents	200	☐	☐	22137	
8	secret	200	☐	☐	73744	
9	secretstuff	200	☐	☐	22162	

Figure 5: Result.

- **Brute Force :**

we will crack the username and password on the Web login. In this method, capture a sample login for a user (hint: enter a name and a password in the login page on your browser and press login) then capture the trace with Burp Suite and send it to Intruder (hint: right click and select: Send to Intruder).

On **Intruder>Positions** page, from **Attack type** drop down menu select: **Cluster bomb**

Then put fuzzifier around username and password only**: $username$, $password$** and clear the rest of fuzzifiers. Then Go to **Intruder>Payloads** page and enter the same user names and passwords in two lists.

Payload set > 1 >

administrator

admin

root

guest

Payload set> 2 >

password

Password

123456

pa$$word

Then run the brute-force fuzzer from the **Intruder>Start Attack** menu on top.

6. Conclusion:

Using Burp Suite tool software platform, we have performed security testing of web applications and analysed web application's attack surface and security vulnerabilities.

Experiment 3: Show Network mapping and port scanning using Nmap tool.

1. Aim: Use Nmap to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc.

2. Objectives: Objective of this module to learn nmap installation & use this to scan different ports.

3. Hardware / Software Required : NMAP Tool

4.Theory:

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.

Nmap features include:

- Host Discovery – Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.
- Port Scanning – Enumerating the open ports on one or more target hosts.
- Version Detection – Interrogating listening network services listening on remote devices to determine the application name and version number.
- OS Detection – Remotely determining the operating system and some hardware characteristics of network devices.

5. Methodology:

Basic commands working in Nmap

For target specifications:

nmap <target's URL or IP with spaces betweenthem>

For OS detection:

nmap -O <target-host's URL orIP>

For version detection:

nmap -sV <target-host's URL orIP>

After the installation of nmap:> **sudo apt-get install nmap**

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections.

FIN scan (-sF)

Sets just the TCP FIN bit.

-sV (Version detection) : Enables version detection, as discussed above. Alternatively, we can use -A, which enables version detection among other things.

-PO protocol list (IP Protocol Ping) :

The newest host discovery option is the IP protocol ping, which sends IP packets with the specified protocol number set in their IP header. The protocol list takes the same format as do port lists in the previously discussed TCP, UDP and SCTP host discovery options.

-p port ranges (Only scan specified ports) .

This option specifies which ports you want to scan and overrides the default. Individual port numbers are OK, as are ranges separated by a hyphen (e.g. 1-1023). The beginning and/or end values of a range may be omitted, causing Nmap to use 1 and 65535, respectively.

-sO (IP protocol scan) .

IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines. This isn´t technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers.

--open (Show only open (or possibly open) ports) .

Sometimes you only care about ports you can actually connect to (open ones), and don´t want results cluttered with closed, filtered, and closed|filtered ports.

-p port ranges (Only scan specified ports) .

This option specifies which ports you want to scan and overrides the default. Individual port numbers are OK, as are ranges separated by a hyphen (e.g. 1-1023). The beginning and/or end values of a range may be omitted, causing Nmap to use 1 and 65535, respectively.

-sT (TCP connect scan) .

TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges or is scanning IPv6 networks. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call. Along with spoofing.

Null scan (-sN):

Does not set any bits (TCP flag header is 0)

--top-ports <integer of 1 or greater>

Scans the N highest-ratio ports found in nmap-services file.

-PS port list (TCP SYN Ping) .

This option sends an empty TCP packet with the SYN flag set. The default destination port is 80 (configurable at compile time by changing DEFAULT_TCP_PROBE_PORT_SPEC innmap.h). Alternate ports can be specified as a parameter. The syntax is the same as for the -p except that port type specifiers like T: are not allowed.

nmap –iflist

host interface and route information with nmap by using ―–iflist‖ option.

6. Conclusion:

Network scanning provides a wealth of information about the target network, which is valuable regardless of whether you're trying to attack the network or protect it from attack. While performing a basic scan is a simple matter, the network scanners covered in this experiment provide a wide array of options to tweak your scan to achieve the best results. Nmap is used to detect IP spoofing and port scanning.

Experiment 4: Implement a code to simulate buffer overflow attack.

1. Aim: Implement a code to simulate buffer overflow attack.

2. Objectives: Objective of the module Is to check buffer overflow in an NS2 environment

3. Hardware / Software Required: Stack Guard compiler.

4. Theory:

A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. This is a special case of the violation of memory safety. A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.

5. Methodology:

Buffer overflow:

Code:

```
#include <stdio.h>
#include <string.h>
int main(void)
{
char buff[15];
int pass = 0;
printf("\n Enter the password : \n");
gets(buff);
if(strcmp(buff, "thecorrectpaswd"))
{
printf ("\n Wrong Password \n");
}
else
{
printf ("\n Correct Password \n");
pass = 1;
}
if(pass)
{
/* Now Give root or admin rights to user*/
printf ("\n Root privileges given to the user \n");
}
return 0;
}
```

Output :

```
>>administrator@cyber:~/Desktop/me CS pracs$ gcc -Wall -fno-stack-protector
bufferoverflow.c -o
>>bufferoverflow
```

The above command deactivates the default GC Compiler's flag which detects Stack Smashing

```
>>administrator@cyber:~/Desktop/me CS pracs$ ./bufferoverflow
>>Enter the password :
thewrong
Wrong Password
```

```
>>administrator@cyber:~/Desktop/me CS pracs$ ./bufferoverflow

>>Enter the password :

thecorrectpaswd

Correct Password

Root privileges given to the user

administrator@cyber:~/Desktop/me CS pracs$ ./bufferoverflow

Enter the password :

thewrongpasswordentered

Wrong Password

Root privileges given to the user
```

Here, the entered password length is above the permissible length with wrong contents still the user is given the ROOT PRIVILEDGES. This demonstrates the Buffer Overflow.

6. Conclusion:

Buffer overflow has been the most exploited vulnerability for more than a decade. Buffer overflow vulnerabilities are the most common way to gain control of a remote host. Attacker can insert and execute attack code. Error is made at program creation, is invisible to user. StackGuard is a systematic compiler tool that prevents a broad class of buffer overflow security attacks from succeeding.

Experiment 5: Demonstrate of Cryptographic algorithm using JCryp tool.

1. Aim: To demonstrate asymmetric, symmetric crypto algorithm using Jcrypt tool.

2. Objectives: To understand Cryptographic algorithm using JCryp tool.

3. Hardware / Software Required: Jcrypt tool software.

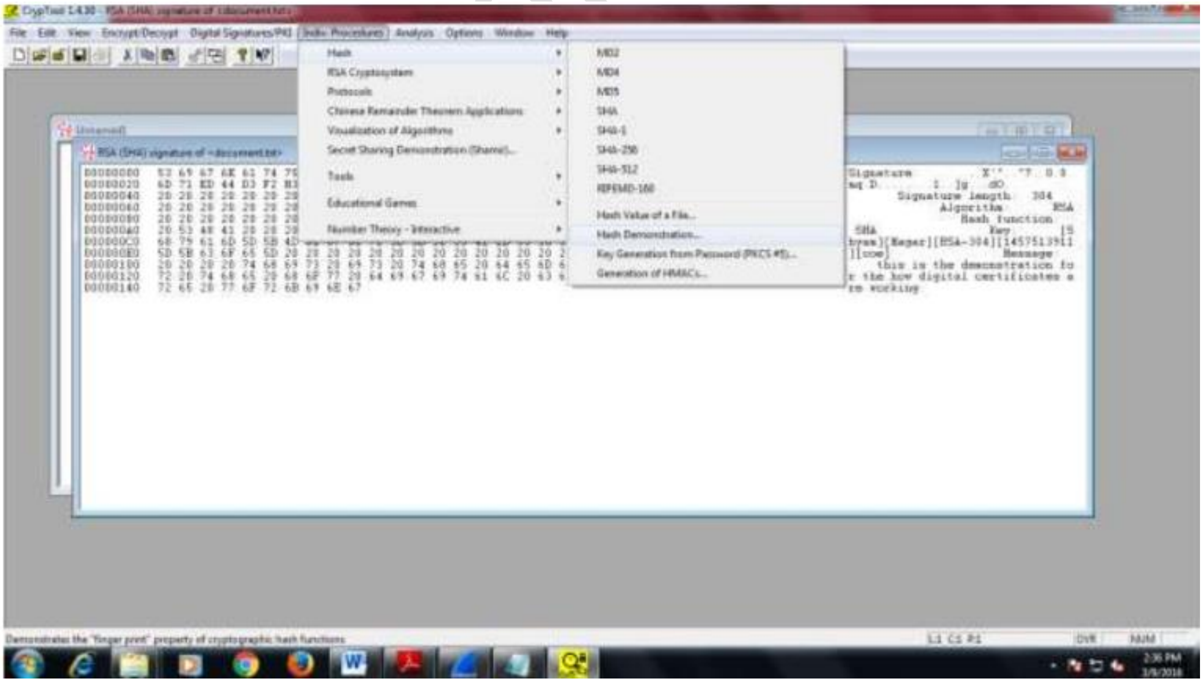
4. Theory:

JCrypTool – abbreviated as JCT – is a free e-learning software for classical and modern cryptology. Cryptology is about techniques and protocols making information available only for authorized persons.The CrypTool project aims to explain and visualize cryptography and cryptanalysis in an easy and understandable way while still being correct from a scientific point of view. Cryptology consists of two parts (fields). The field cryptography: Science of encryption systems guaranteeing secure and confidential storage and exchange of information (e.g. between computers). The field cryptanalysis : Cryptanalysis is the counter part to cryptography and studies theories and techniques for testing and breaking cryptographic methods.

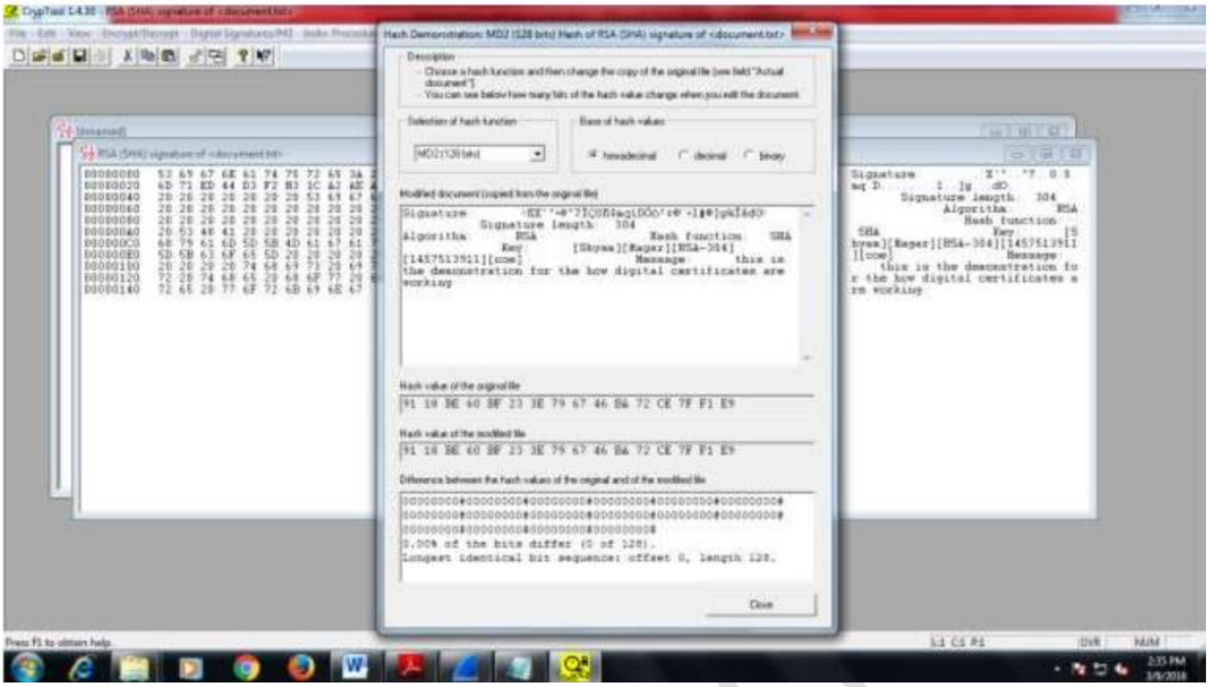
5. Methodology:

a)Hash Function

1. Select Indiv. Procedure → Hash → Hash Demonstration


CrypTool 1.4.30 - RSA (SHA) signature of <document.txt>
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Window
Help
Hash
RSA Cryptosystem
Protocols
Chinese Remainder Theorem Applications
Visualization of Algorithms
Secret Sharing Demonstration (Shamir)...
Tools
Educational Games
Number Theory - Interactive
MD2
MD4
MD5
SHA
SHA-1
SHA-256
SHA-512
RIPEMD-160
Hash Value of a File...
Hash Demonstration...
Key Generation from Password (PKCS #5)...
Generation of HMACs...
Unnamed1
RSA (SHA) signature of <document.txt>
Demonstrates the "finger print" property of cryptographic hash functions

2. Selection of hash Function



Hash Demonstration: MD2 (128 bits) Hash of RSA (SHA) signature of <document.txt>

Description
- Choose a hash function and then change the copy of the original file (see field "Actual document")
- You can see below how many bits of the hash value change when you edit the document

Selection of hash function: MD2 (128 bits)

Base of hash values: ● hexadecimal ○ decimal ○ binary

Modified document (copied from the original file)

```
Signature        ·EE'`-Φ'7IÇ0ß4ŒgiDÕò'¢Φ ·1‡Φ]gÑÏäðÞ
           Signature length   304
Algorithm       RSA                  Hash function    SHA
          Key         [Shyam][Nagar][RSA-304]
[1457513911][com]                   Message       this is
the demonstration for the how digital certificates are
working
```

Hash value of the original file

```
91 18 BE 60 BF 23 3E 79 67 46 BA 72 CE 7F F1 E9
```

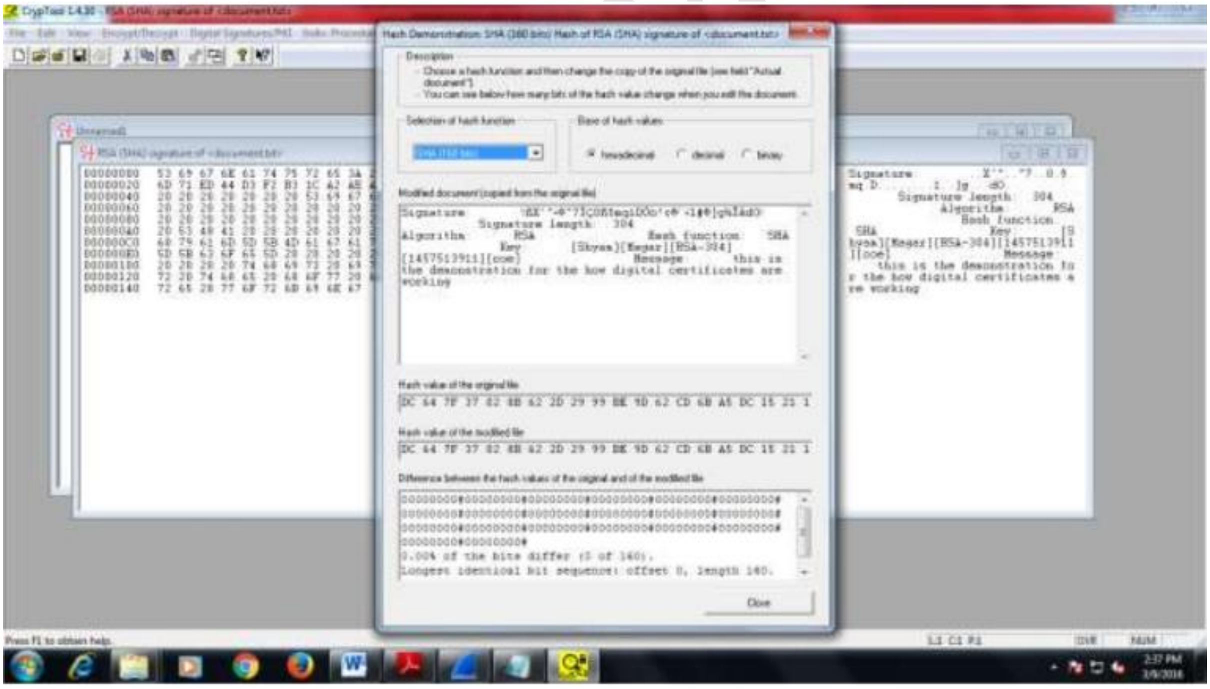
Hash value of the modified file

```
91 18 BE 60 BF 23 3E 79 67 46 BA 72 CE 7F F1 E9
```

Difference between the hash values of the original and of the modified file

```
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#00000000#00000000#
0.00% of the bits differ (0 of 128).
Longest identical bit sequence: offset 0, length 128.
```

3. Select hash function SHA you get hash code value



Hash Demonstration: SHA (160 bits) Hash of RSA (SHA) signature of <document.txt>

Description
- Choose a hash function and then change the copy of the original file (see field "Actual document")
- You can see below how many bits of the hash value change when you edit the document

Selection of hash function: SHA (160 bits)

Base of hash values: ● hexadecimal ○ decimal ○ binary

Modified document (copied from the original file)

```
Signature        ·EE'`-Φ'7IÇ0ß4ŒgiDÕò'¢Φ ·1‡Φ]gÑÏäðÞ
           Signature length   304
Algorithm       RSA                  Hash function    SHA
          Key         [Shyam][Nagar][RSA-304]
[1457513911][com]                   Message       this is
the demonstration for the how digital certificates are
working
```

Hash value of the original file

```
DC 64 7F 37 82 8B 62 2D 29 99 BE 9D 62 CD 6B A5 DC 15 21 1
```

Hash value of the modified file

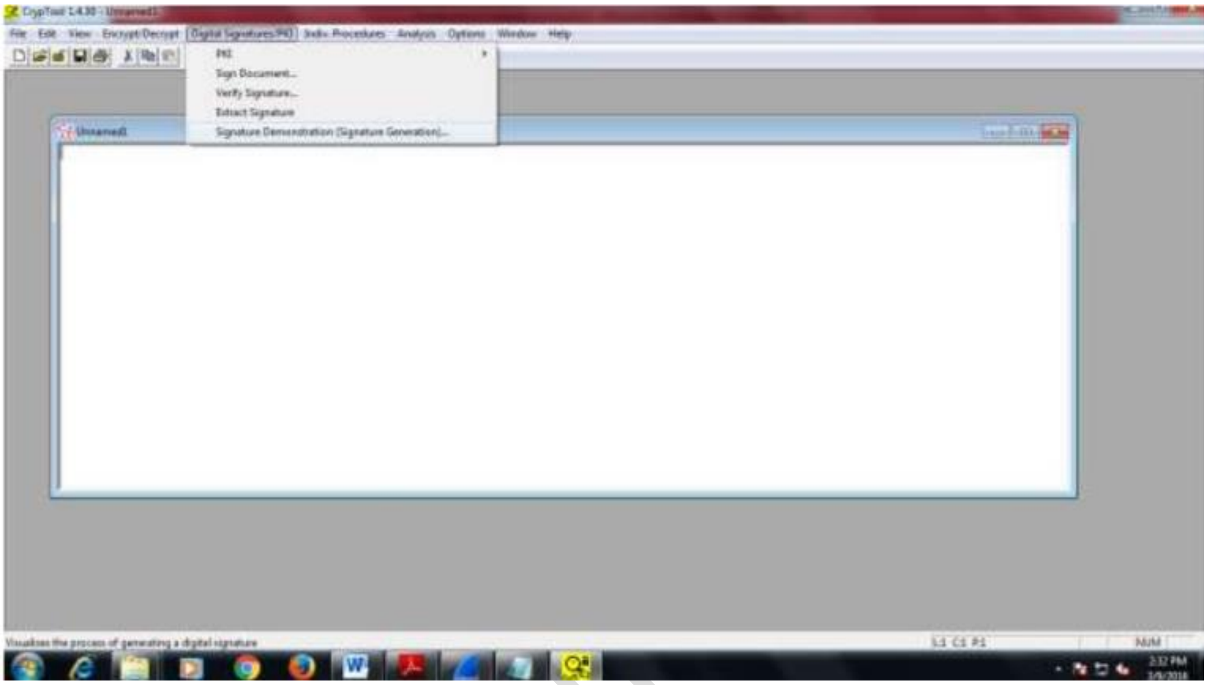
```
DC 64 7F 37 82 8B 62 2D 29 99 BE 9D 62 CD 6B A5 DC 15 21 1
```

Difference between the hash values of the original and of the modified file

```
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#
0.00% of the bits differ (0 of 160).
Longest identical bit sequence: offset 0, length 160.
```

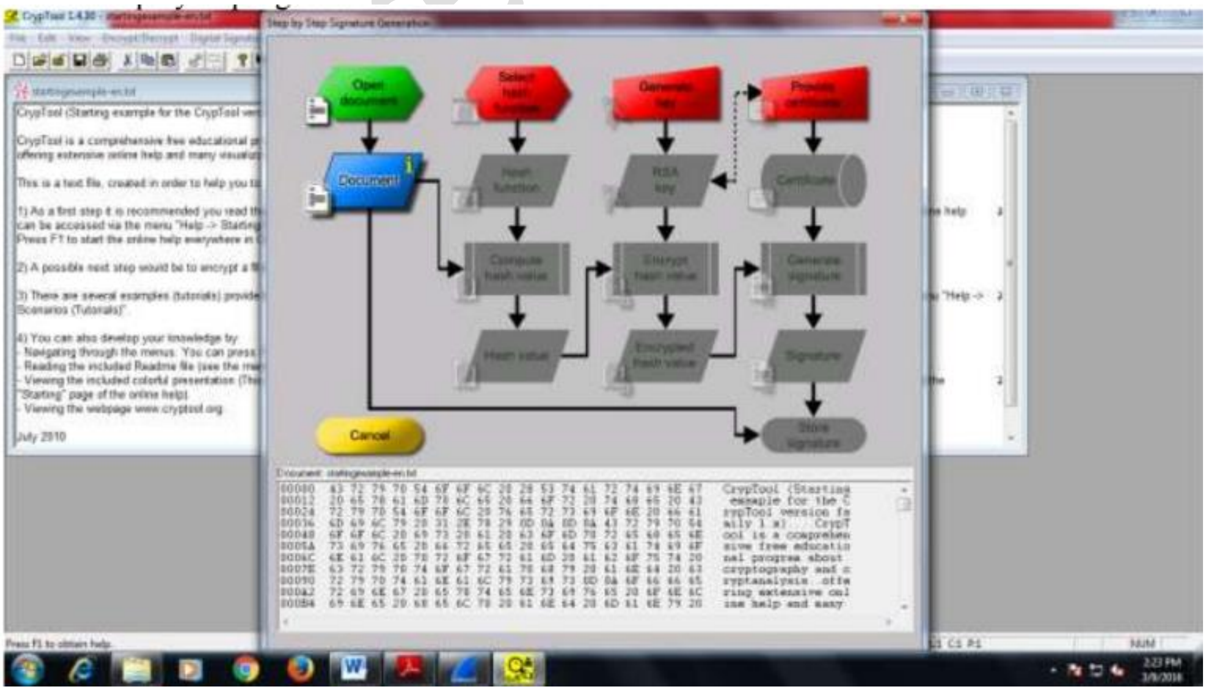
(b) Digital Signatures

1. Select Digital Signature menu → signature demonstration



Visualizes the process of generating a digital signature

2. Step by step signature



startingexample-en.txt

CrypTool (Starting example for the CrypTool ver

CrypTool is a comprehensive free educational p
offering extensive online help and many visualiz

This is a text file, created in order to help you t

1) As a first step it is recommended you read th
can be accessed via the menu "Help -> Starting
Press F1 to start the online help everywhere in C

2) A possible next step would be to encrypt a fi

3) There are several examples (tutorials) provide
Scenarios (Tutorials)".

4) You can also develop your knowledge by
- Navigating through the menus. You can press
- Reading the included Readme file (see the me
- Viewing the included colorful presentation (Th
"Starting" page of the online help)
- Viewing the webpage www.cryptool.org

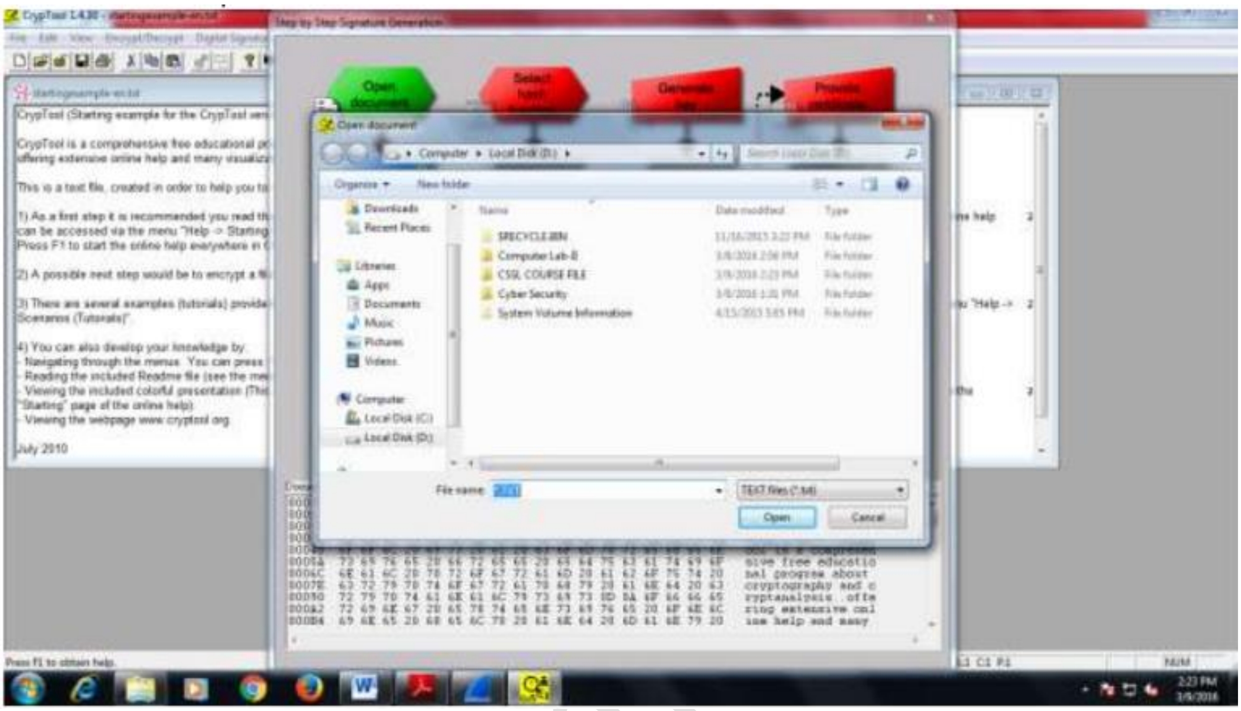
July 2010

Document: startingexample-en.txt

```
00000  43 72 79 70 54 6F 6F 6C 20 28 53 74 61 72 74 69 6E 67   CrypTool (Starting
00012  20 65 78 61 6D 70 6C 65 20 66 6F 72 20 74 68 65 20 43    example for the C
00024  72 79 70 54 6F 6F 6C 20 76 65 72 73 69 6F 6E 20 66 61   rypTool version fa
00036  6D 69 6C 79 20 31 2E 78 29 0D 0A 0D 0A 43 72 79 70 54   mily 1.x)....CrypT
00048  6F 6F 6C 20 69 73 20 61 20 63 6F 6D 70 72 65 68 65 6E   ool is a comprehen
0005A  73 69 76 65 20 66 72 65 65 20 65 64 75 63 61 74 69 6F   sive free educatio
0006C  6E 61 6C 20 70 72 6F 67 72 61 6D 20 61 62 6F 75 74 20   nal program about 
0007E  63 72 79 70 74 6F 67 72 61 70 68 79 20 61 6E 64 20 63   cryptography and c
00090  72 79 70 74 61 6E 61 6C 79 73 69 73 0D 0A 6F 66 66 65   ryptanalysis..offe
000A2  72 69 6E 67 20 65 78 74 65 6E 73 69 76 65 20 6F 6E 6C   ring extensive onl
000B4  69 6E 65 20 68 65 6C 70 20 61 6E 64 20 6D 61 6E 79 20   ine help and many 
```

Press F1 to obtain help.

3. Click on open document & select txt file



Name	Date modified	Type
$RECYCLE.BIN	11/16/2013 3:22 PM	File folder
Computer Lab-II	3/8/2016 2:08 PM	File folder
CSSL COURSE FILE	3/9/2016 2:23 PM	File folder
Cyber Security	3/8/2016 1:31 PM	File folder
System Volume Information	4/15/2013 3:03 PM	File folder

File name:

TEXT files (*.txt)

CrypTool (Starting example for the CrypTool ver

CrypTool is a comprehensive free educational pr
offering extensive online help and many visualiz

This is a text file, created in order to help you to

1) As a first step it is recommended you read th
can be accessed via the menu "Help -> Starting
Press F1 to start the online help everywhere in C

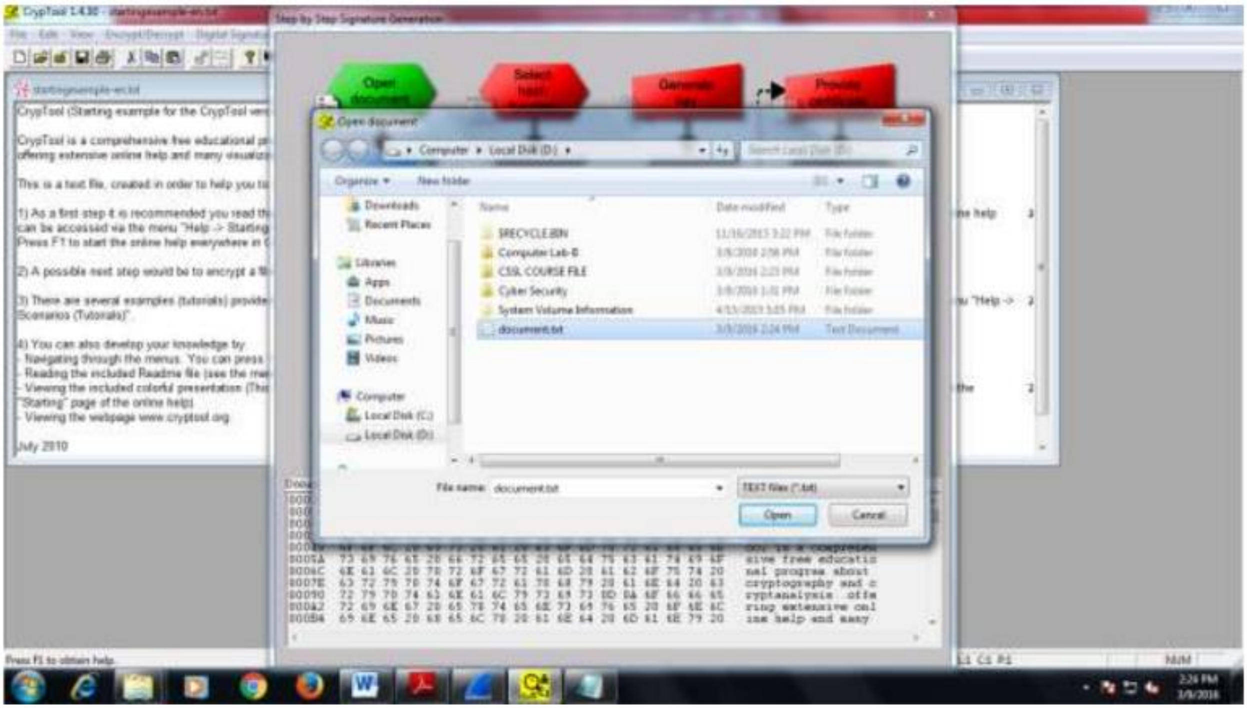
2) A possible next step would be to encrypt a fil

3) There are several examples (tutorials) provide
Scenarios (Tutorials)".

4) You can also develop your knowledge by:
- Navigating through the menus. You can press
- Reading the included Readme file (see the me
- Viewing the included colorful presentation (Thi
"Starting" page of the online help)
- Viewing the webpage www.cryptool.org

July 2010

```
0005A  73 69 76 65 20 66 72 65 65 20 65 64 75 63 61 74 69 6F   sive free educatio
0006C  6E 61 6C 20 70 72 6F 67 72 61 6D 20 61 62 6F 75 74 20   nal program about
0007E  63 72 79 70 74 6F 67 72 61 70 68 79 20 61 6E 64 20 63   cryptography and c
00090  72 79 70 74 61 6E 61 6C 79 73 69 73 0D 0A 6F 66 66 65   ryptanalysis..offe
000A2  72 69 6E 67 20 65 78 74 65 6E 73 69 76 65 20 6F 6E 6C   ring extensive onl
000B4  69 6E 65 20 68 65 6C 70 20 61 6E 64 20 6D 61 6E 79 20   ine help and many
```

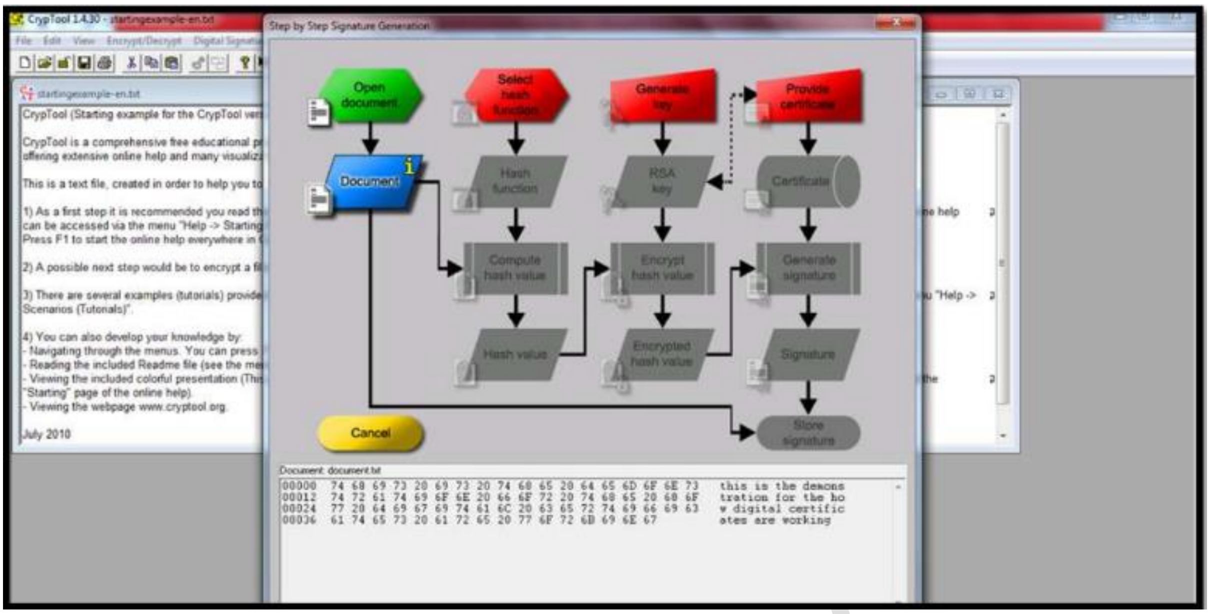


Name	Date modified	Type
$RECYCLE.BIN	11/16/2013 3:22 PM	File folder
Computer Lab-II	3/8/2016 2:08 PM	File folder
CSSL COURSE FILE	3/9/2016 2:23 PM	File folder
Cyber Security	3/8/2016 1:31 PM	File folder
System Volume Information	4/15/2013 3:03 PM	File folder
document.txt	3/9/2016 2:24 PM	Text Document

File name: document.txt

TEXT files (*.txt)

4. Document is converted in to hexadecimal value & ready to compute hash value



CrypTool (Starting example for the CrypTool ver

CrypTool is a comprehensive free educational p
offering extensive online help and many visualiz

This is a text file, created in order to help you to

1) As a first step it is recommended you read th
can be accessed via the menu "Help -> Starting
Press F1 to start the online help everywhere in

2) A possible next step would be to encrypt a fi

3) There are several examples (tutorials) provide
Scenarios (Tutorials)".

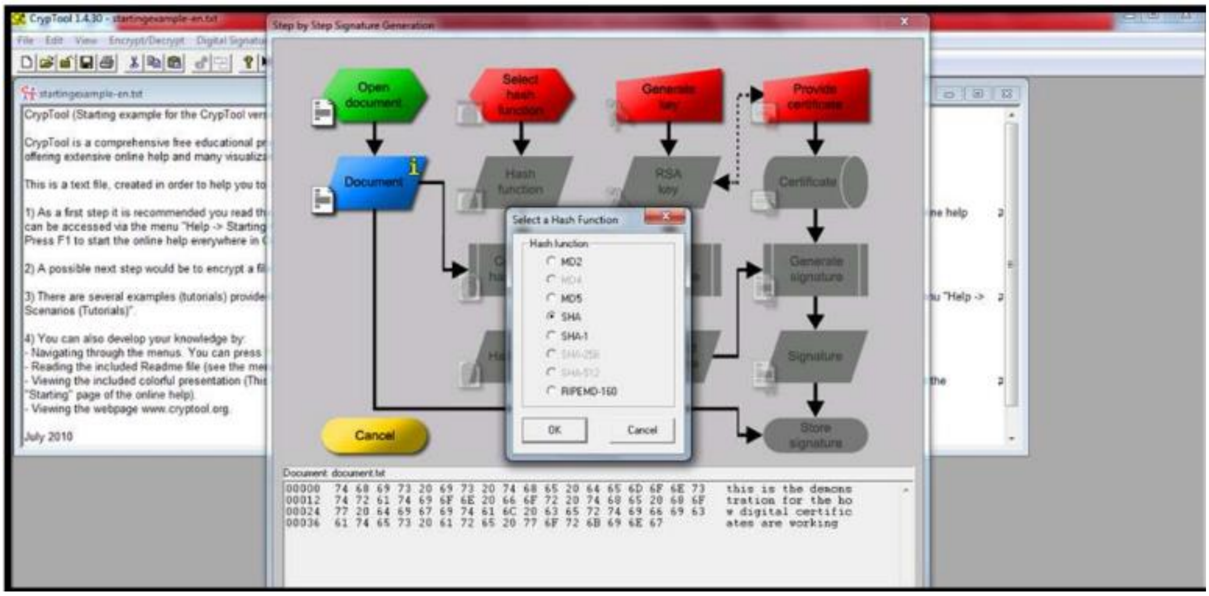
4) You can also develop your knowledge by:
- Navigating through the menus. You can press
- Reading the included Readme file (see the me
- Viewing the included colorful presentation (Thi
"Starting" page of the online help).
- Viewing the webpage www.cryptool.org.

July 2010

Document: document.txt

```
00000  74 68 69 73 20 69 73 20 74 68 65 20 64 65 6D 6F 6E 73   this is the demons
00012  74 72 61 74 69 6F 6E 20 66 6F 72 20 74 68 65 20 68 6F   tration for the ho
00024  77 20 64 69 67 69 74 61 6C 20 63 65 72 74 69 66 69 63   w digital certific
00036  61 74 65 73 20 61 72 65 20 77 6F 72 6B 69 6E 67         ates are working
```

5. Select Hash function from given list as SHA



Select a Hash Function

Hash function

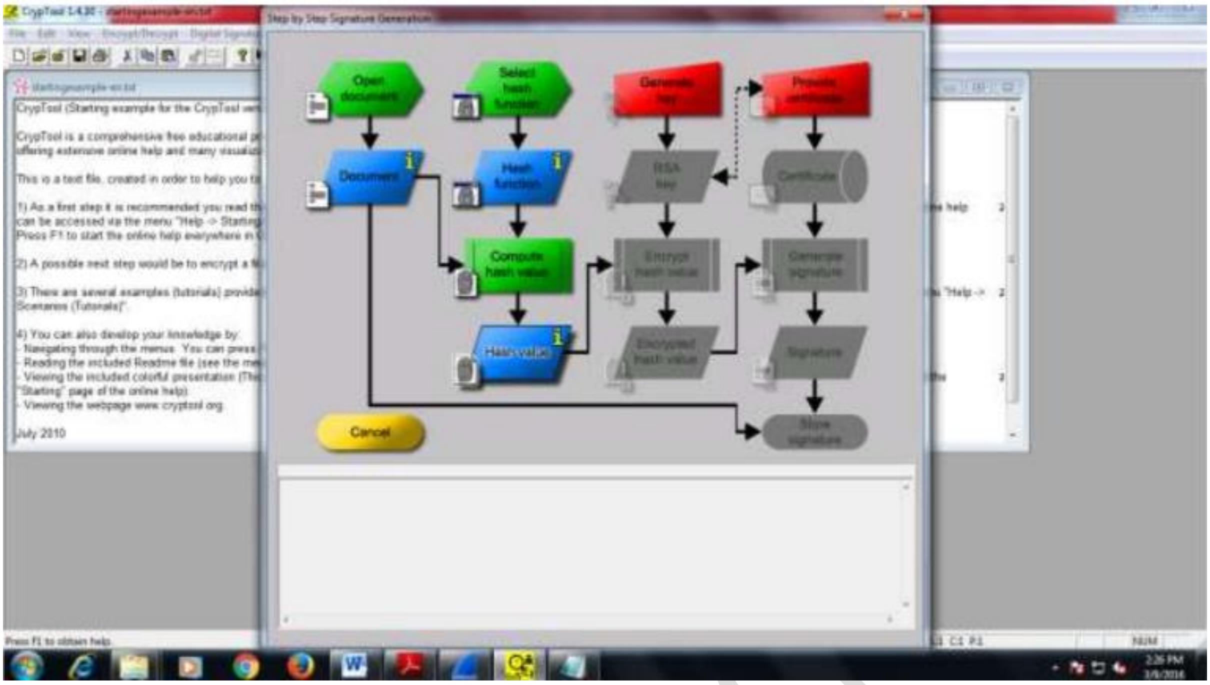
○ MD2
○ MD4
○ MD5
● SHA
○ SHA-1
○ SHA-256
○ SHA-512
○ RIPEMD-160

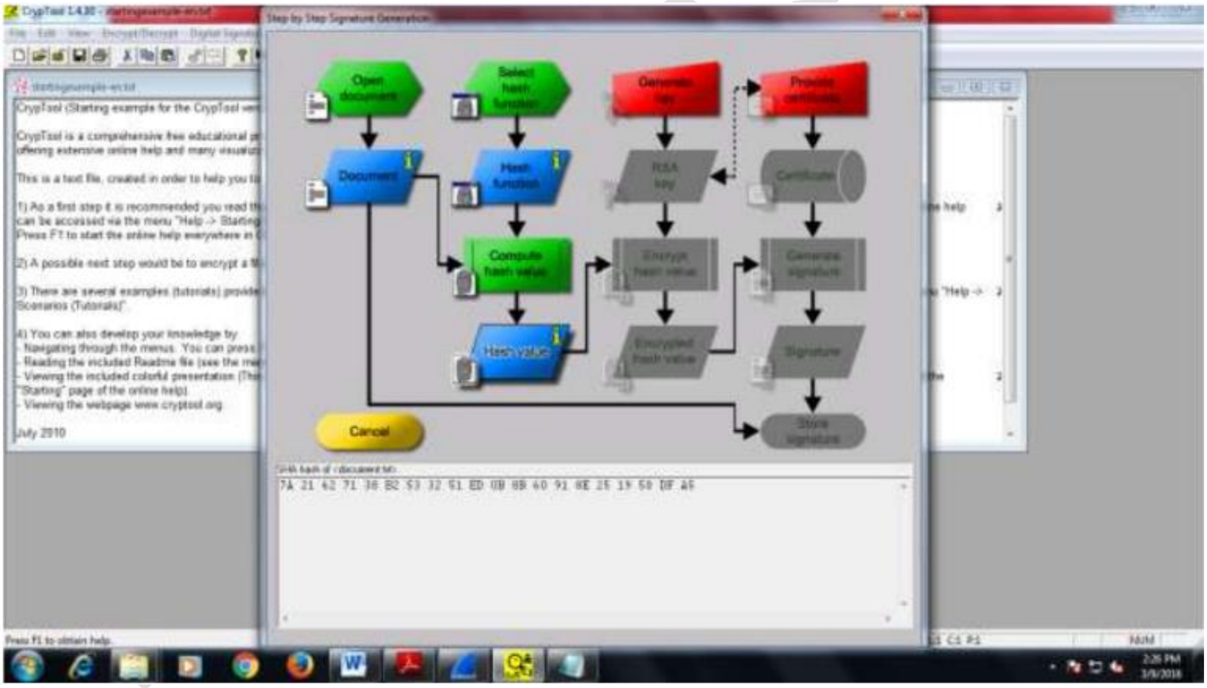
OK Cancel

Document: document.txt

```
00000  74 68 69 73 20 69 73 20 74 68 65 20 64 65 6D 6F 6E 73   this is the demons
00012  74 72 61 74 69 6F 6E 20 66 6F 72 20 74 68 65 20 68 6F   tration for the ho
00024  77 20 64 69 67 69 74 61 6C 20 63 65 72 74 69 66 69 63   w digital certific
00036  61 74 65 73 20 61 72 65 20 77 6F 72 6B 69 6E 67         ates are working
```

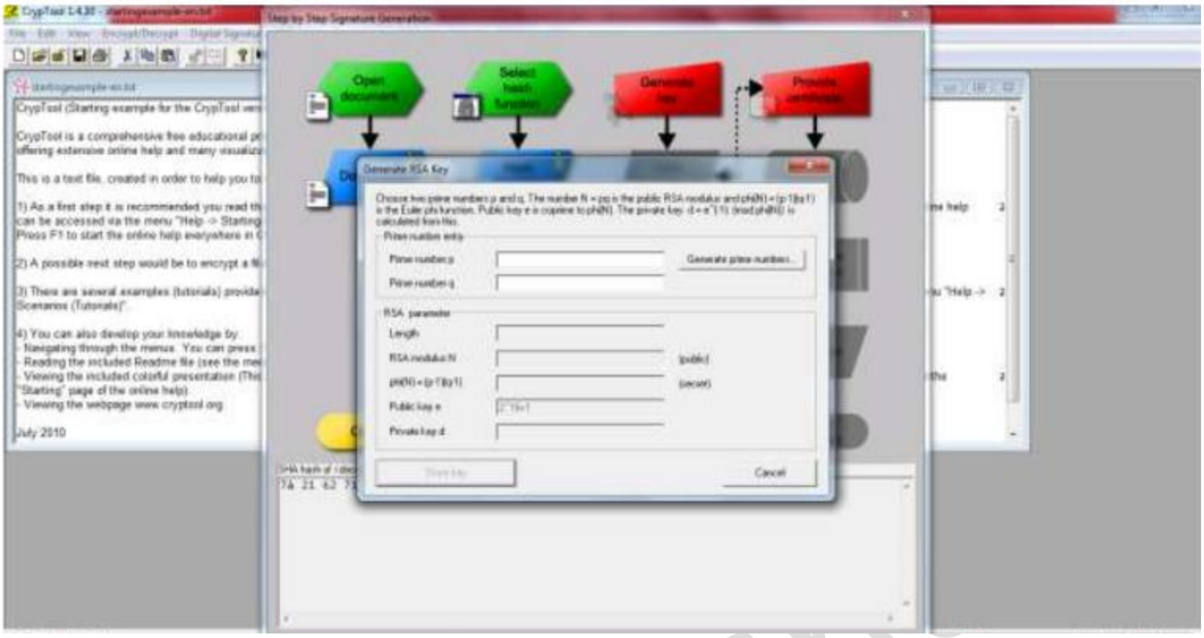
6.Click on compute hash value & hash value you will get the hash value





```
SHA hash of <document.txt>
7A 21 62 71 38 B2 53 32 51 ED 0B 8B 60 91 8E 25 19 58 DF A5
```

7.Click on generate key & provide P & Q value for generating prime no



Generate RSA Key

Choose two prime numbers p and q. The number N = pq is the public RSA modulus and phi(N) = (p-1)(q-1) is the Euler phi function. Public key e is coprime to phi(N). The private key d = e^(-1) (mod phi(N)) is calculated from this.

Prime number entry

Prime number p

Prime number q

RSA parameter

Length

RSA modulus N (public)

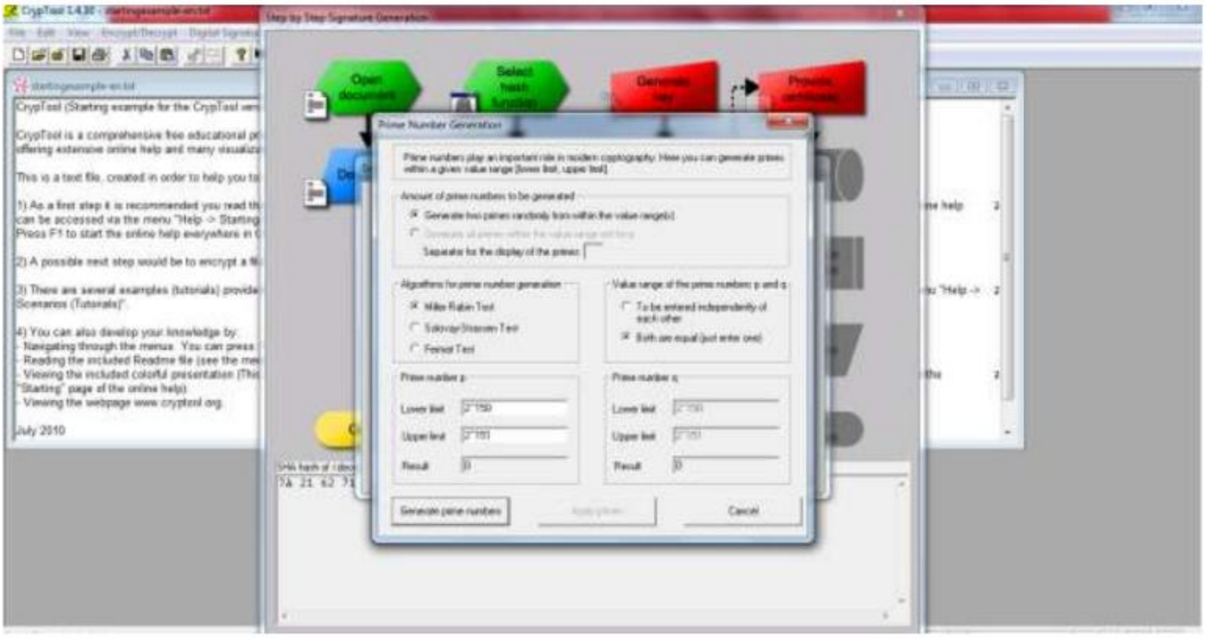
phi(N) = (p-1)(q-1) (secret)

Public key e: 2^16+1

Private key d

CrypTool 1.4.30 - startingexample-en.txt
Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate
Generate prime numbers...
Store key
Cancel

8. Generate prime no according to algorithm



Prime Number Generation

Prime numbers play an important role in modern cryptography. Here you can generate primes within a given value range [lower limit, upper limit]

Amount of prime numbers to be generated

● Generate two primes randomly from within the value range(s)

○ Generate all primes within the value range and listing

Separator for the display of the primes:

Algorithms for prime number generation

● Miller-Rabin Test

○ Solovay-Strassen Test

○ Fermat Test

Value range of the prime numbers p and q

○ To be entered independently of each other

● Both are equal (just enter one)

Prime number p

Lower limit: 2^150

Upper limit: 2^151

Result: 0

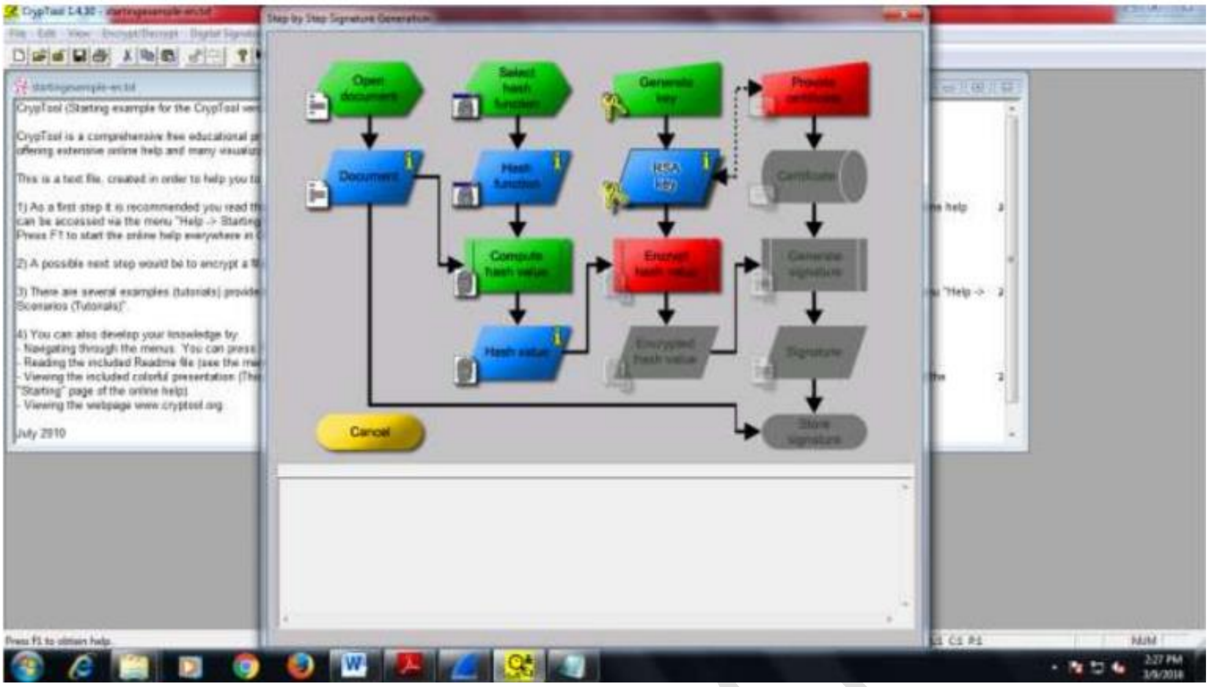
Prime number q

Lower limit: 2^150

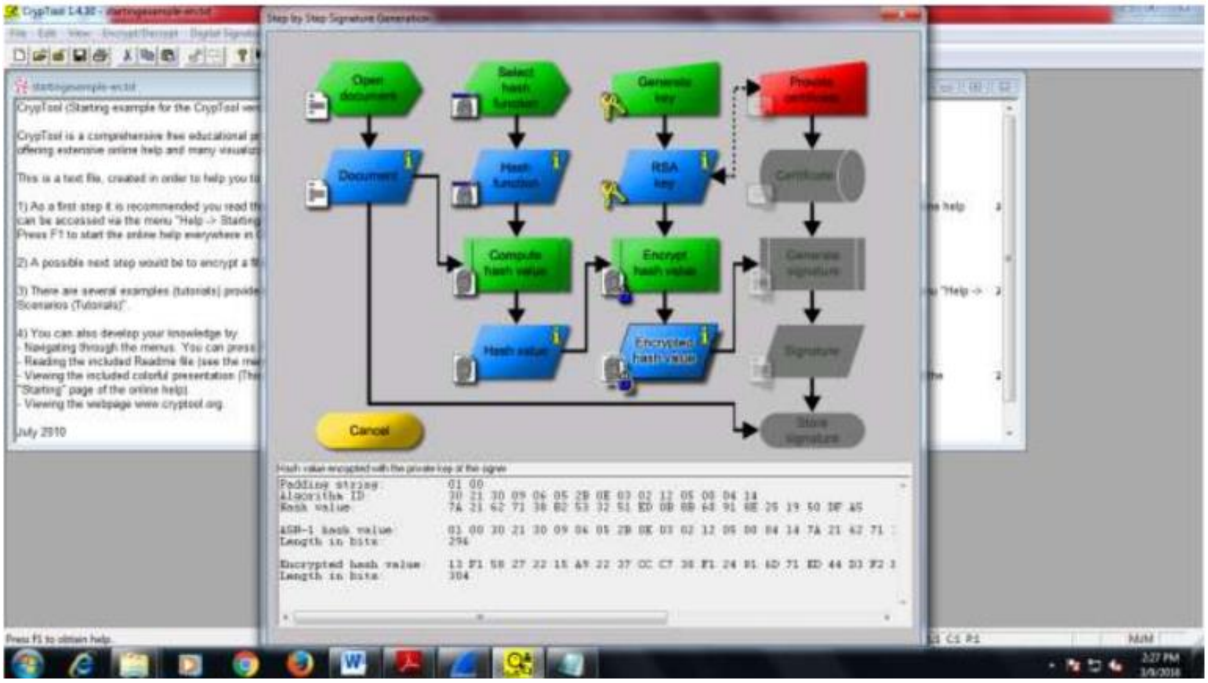
Upper limit: 2^151

Result: 0

10. Generate the RSA key & click on encrypt hash value



11.Check Encrypted HashValue



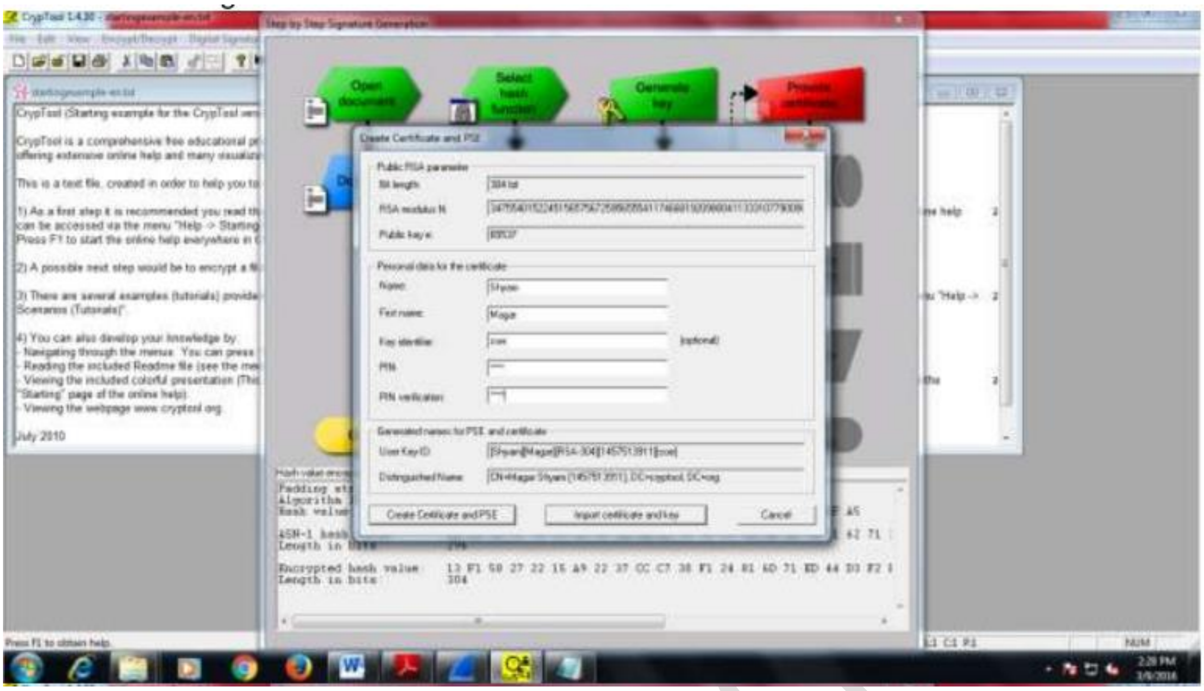
Hash value encrypted with the private key of the signer

```
Padding string        01 00
Algorithm ID          30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14
Hash value            7A 21 62 71 38 B2 53 32 51 ED 0B 8B 68 91 8E 25 19 50 DF A5

ASN-1 hash value      01 00 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14 7A 21 62 71
Length in bits        296

Encrypted hash value  13 F1 58 27 22 15 A9 22 37 CC C7 38 F1 24 B1 6D 71 ED 44 D3 F2 3
Length in bits        304
```

12. Provide Digital Certificate



CrypTool 1.4.30 - startingexample-en.txt
Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate

Create Certificate and PSE

Public RSA parameter

- Bit length: 304 bit
- RSA modulus N: 3475540152245156575672589; [illegible]
- Public key e: 65537

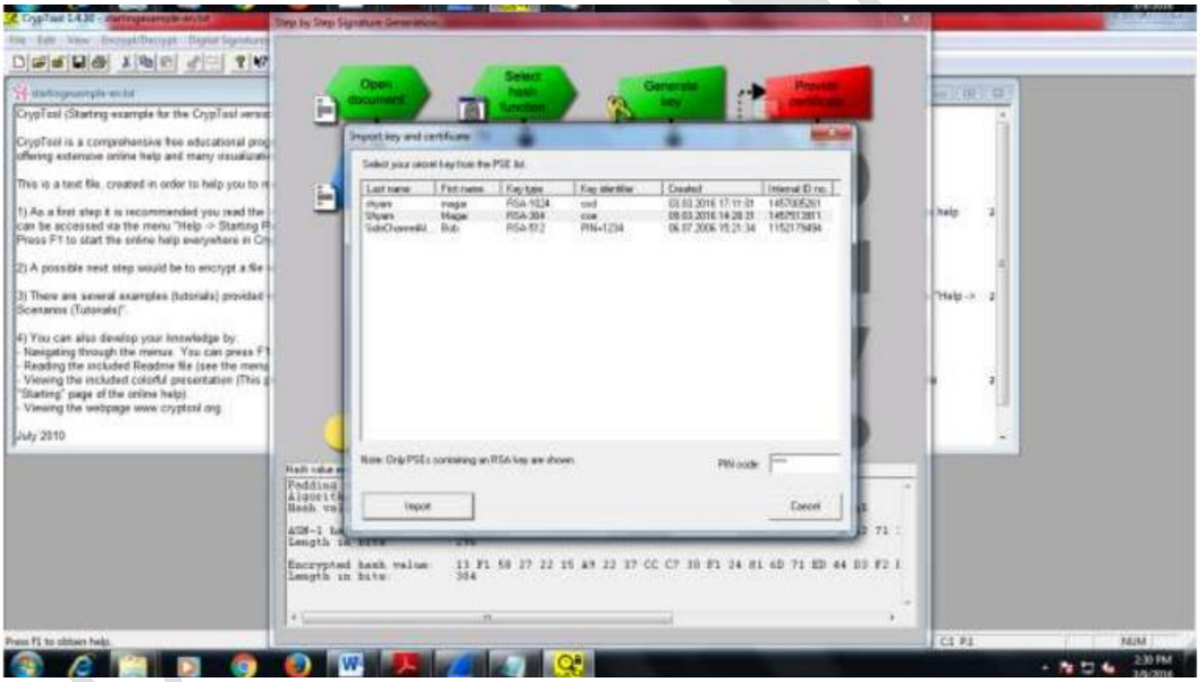
Personal data for the certificate

- Name: Shyam
- First name: Magar
- Key identifier: coe (optional)
- PIN: ****
- PIN verification: ****

Generated names for PSE and certificate

- User Key ID: [Shyam][Magar][RSA-304][1457513911][coe]
- Distinguished Name: CN=Magar Shyam [1457513911], DC=cryptool, DC=org

```
Encrypted hash value:   13 F1 58 27 22 15 A9 22 37 CC C7 38 F1 24 81 6D 71 ED 44 D3 F2
Length in bits:         304
```



CrypTool 1.4.30 - startingexample-en.txt
Step by Step Signature Generation
Open document
Select hash function
Generate key
Provide certificate

Import key and certificate

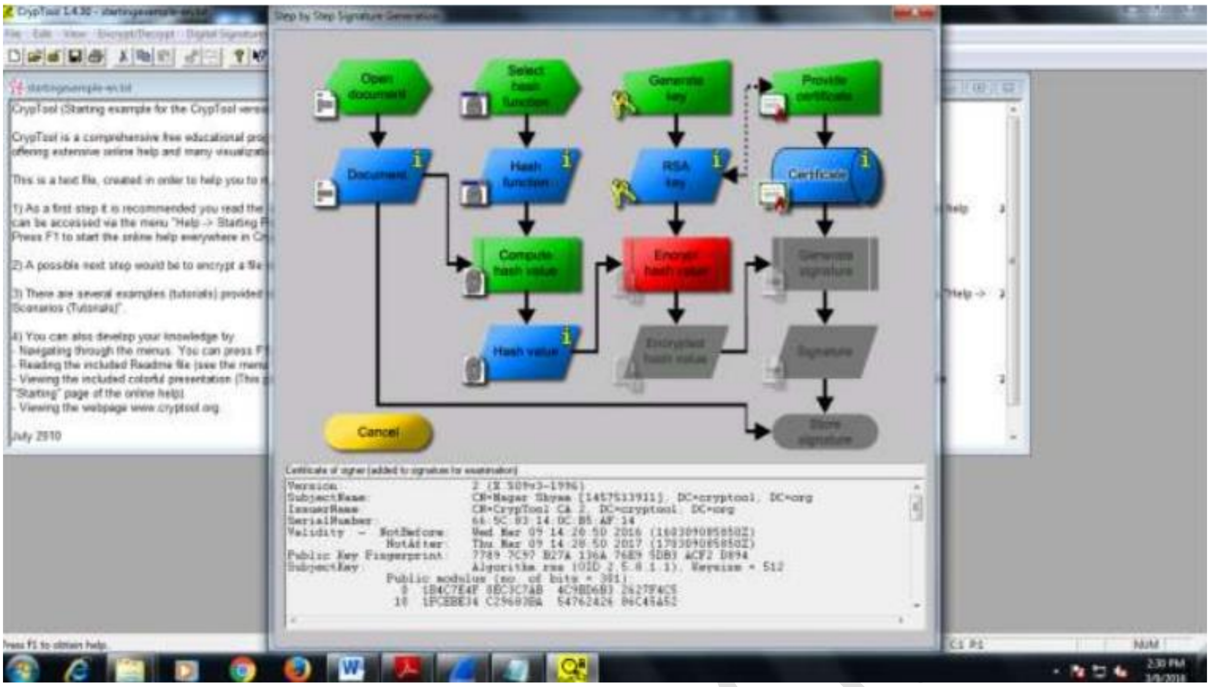
Select your secret key from the PSE list:

Last name	First name	Key type	Key identifier	Created	Internal ID no.
shyam	magar	RSA-1024	ccd	03.03.2016 17:11:01	1457005261
Shyam	Magar	RSA-304	coe	09.03.2016 14:28:31	1457513811
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 15:21:34	1152179494

Note: Only PSEs containing an RSA key are shown.

PIN code: ****

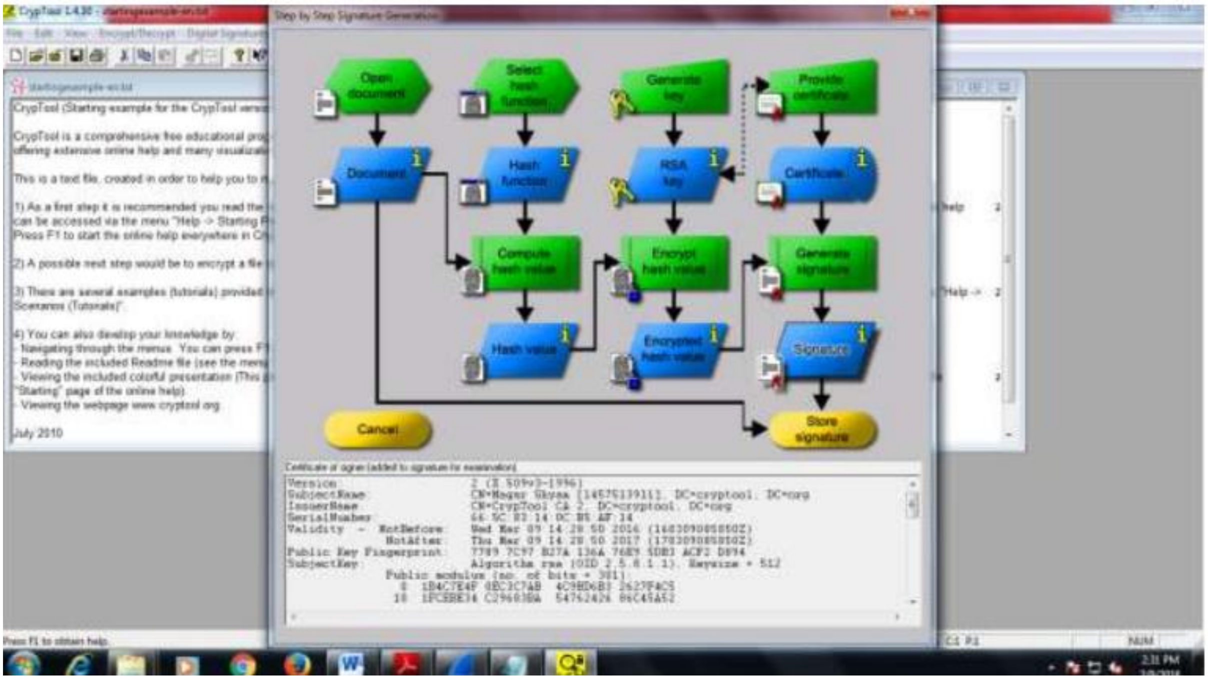
```
Encrypted hash value:   13 F1 58 27 22 15 A9 22 37 CC C7 38 F1 24 81 6D 71 ED 44 D3 F2
Length in bits:         304
```



Certificate of signer (added to signature for examination)

```
Version:                      2 (X.509v3-1996)
SubjectName:                  CN=Nagar Shyam [1457513911], DC=cryptool, DC=org
IssuerName:                   CN=CrypTool CA 2, DC=cryptool, DC=org
SerialNumber:                 66 5C 03 14 DC B5 AF 14
Validity  -  NotBefore:       Wed Mar 09 14:20:50 2016 (160309085050Z)
             NotAfter:        Thu Mar 09 14:20:50 2017 (170309085050Z)
Public Key Fingerprint:       7789 7C97 B27A 136A 76E9 5DB3 ACF2 D894
SubjectKey:                   Algorithm rsa (OID 2.5.8.1.1), Keysize = 512
             Public modulus (no. of bits = 381):
               0  1B4C7E4F 8EC3C7AB  4C9BD6B3 2627F4C5
              10  1FCEBE34 C29603BA  54762424 86C45A52
```

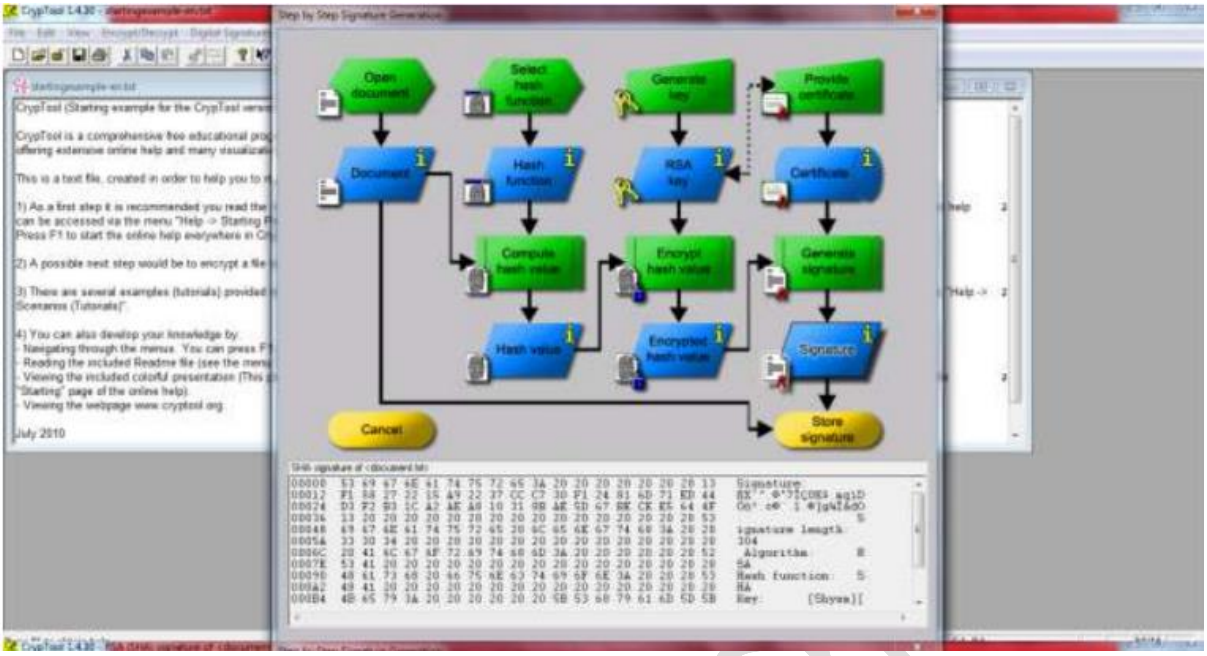
13. Generate Certificate & Signature

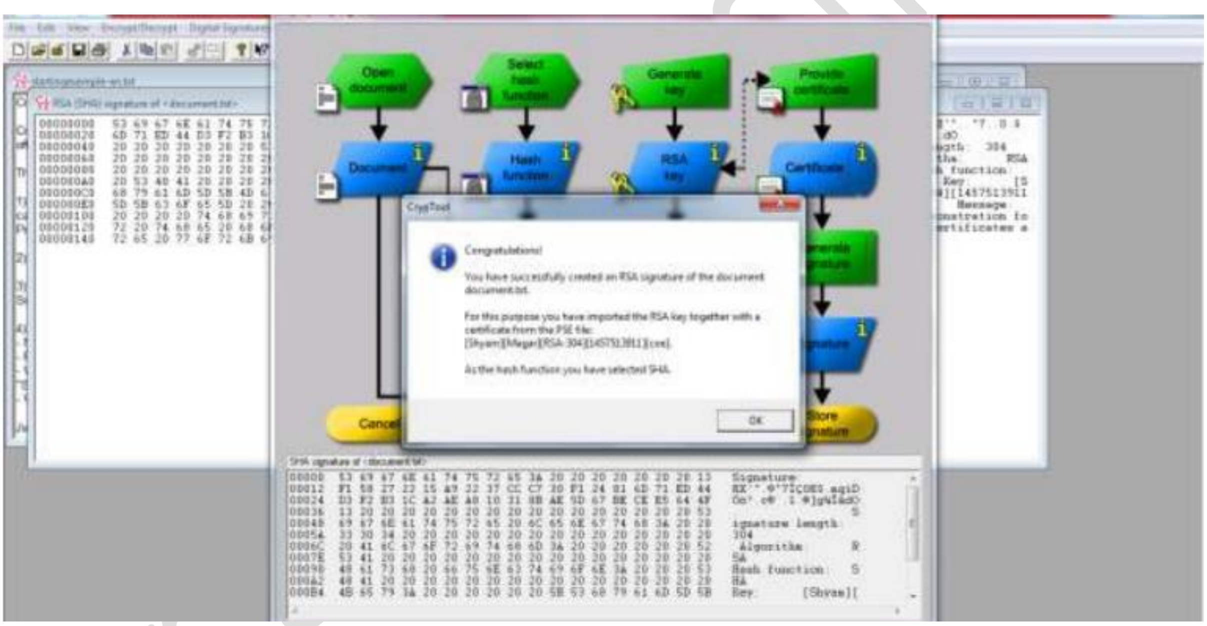


Certificate of signer (added to signature for examination)

```
Version:                      2 (X.509v3-1996)
SubjectName:                  CN=Nagar Shyam [1457513911], DC=cryptool, DC=org
IssuerName:                   CN=CrypTool CA 2, DC=cryptool, DC=org
SerialNumber:                 66 5C 03 14 DC B5 AF 14
Validity  -  NotBefore:       Wed Mar 09 14:20:50 2016 (160309085050Z)
             NotAfter:        Thu Mar 09 14:20:50 2017 (170309085050Z)
Public Key Fingerprint:       7789 7C97 B27A 136A 76E9 5DB3 ACF2 D894
SubjectKey:                   Algorithm rsa (OID 2.5.8.1.1), Keysize = 512
             Public modulus (no. of bits = 381):
               0  1B4C7E4F 8EC3C7AB  4C9BD6B3 2627F4C5
              10  1FCEBE34 C29603BA  54762424 86C45A52
```

14. Check the Digital Signature & Store the Signature



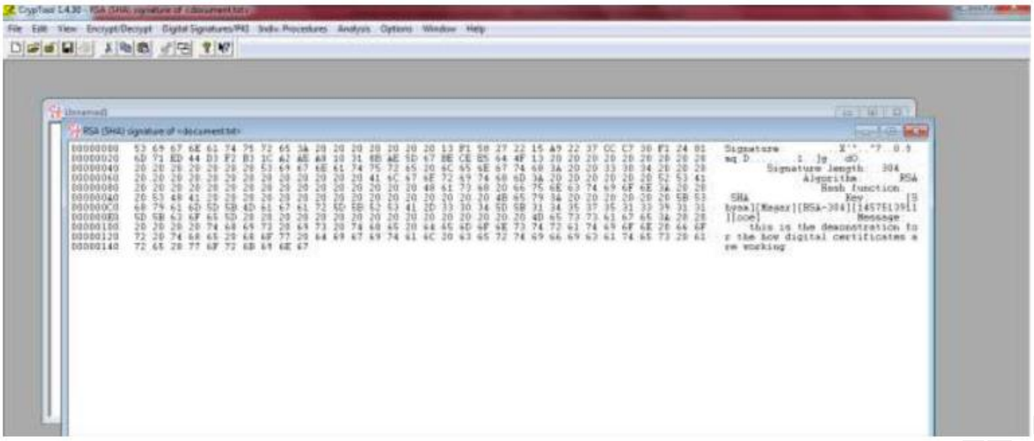


Congratulations!

You have successfully created an RSA signature of the document document.txt.

For this purpose you have imported the RSA key together with a certificate from the PSE file: [Shyam][Megan][RSA-304][1457513811][.cse].

As the hash function you have selected SHA.


CrypTool 1.4.30 - RSA (SHA) signature of <document.txt>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed1
RSA (SHA) signature of <document.txt>

```
00000000   53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 13 F1 58 27 22 15 A9 22 37 CC C7 30 F1 24 01   Signature:        X'"..'7..0.$.
00000020   6D 71 ED 44 D3 F2 B3 1C A2 AE A8 10 31 8B AE 5D 67 BE CE E5 64 4F 13 20 20 20 20 20 20 20 20 20   mq.D........1..]g...dO.
00000040   20 20 20 20 20 20 20 53 69 67 6E 61 74 75 72 65 20 6C 65 6E 67 74 68 3A 20 20 33 30 34 20 20 20          Signature length:  304
00000060   20 20 20 20 20 20 20 20 20 20 20 20 20 41 6C 67 6F 72 69 74 68 6D 3A 20 20 20 20 20 20 52 53 41                Algorithm:      RSA
00000080   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 48 61 73 68 20 66 75 6E 63 74 69 6F 6E 3A 20 20                   Hash function:
000000A0   20 53 48 41 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 4B 65 79 3A 20 20 20 20 20 20 5B 53    SHA                Key:      [S
000000C0   68 79 61 6D 5D 5B 4D 61 67 61 72 5D 5B 52 53 41 2D 33 30 34 5D 5B 31 34 35 37 35 31 33 39 31 31   hyam][Magar][RSA-304][1457513911
000000E0   5D 5B 63 6F 65 5D 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 4D 65 73 73 61 67 65 3A 20 20   ][coe]                Message:
00000100   20 20 20 20 74 68 69 73 20 69 73 20 74 68 65 20 64 65 6D 6F 6E 73 74 72 61 74 69 6F 6E 20 66 6F       this is the demonstration fo
00000120   72 20 74 68 65 20 68 6F 77 20 64 69 67 69 74 61 6C 20 63 65 72 74 69 66 69 63 61 74 65 73 20 61   r the how digital certificates a
00000140   72 65 20 77 6F 72 6B 69 6E 67                                                                     re working
```

6. Conclusion: Hence we demonstrated asymmetric, symmetric crypto algorithm using Jcrypt tool.

Experiment 6: Demonstrate Network reconnaissance using WHOIS tool.

1. Aim: To demonstrate Network reconnaissance using WHOIS tool.

2. Objectives: To know how to gather information about the networks by using network reconnaissance tools.

3. Hardware / Software Required: WHOIS client

4. Theory:

Reconnaissance is the gathering of information about a target prior to launching an attack. Most attacks begin by gathering as much information as possible about the target. The whois databases are a set of tools that can be used for reconnaissance, and are one of the best sets of tools available. They can be used to get detailed information about a domain, and can help you gather information about a target. Whois - whois searches for an object in a WHOIS database. WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block, but is also used for a wider range of other information.

5. Methodology:

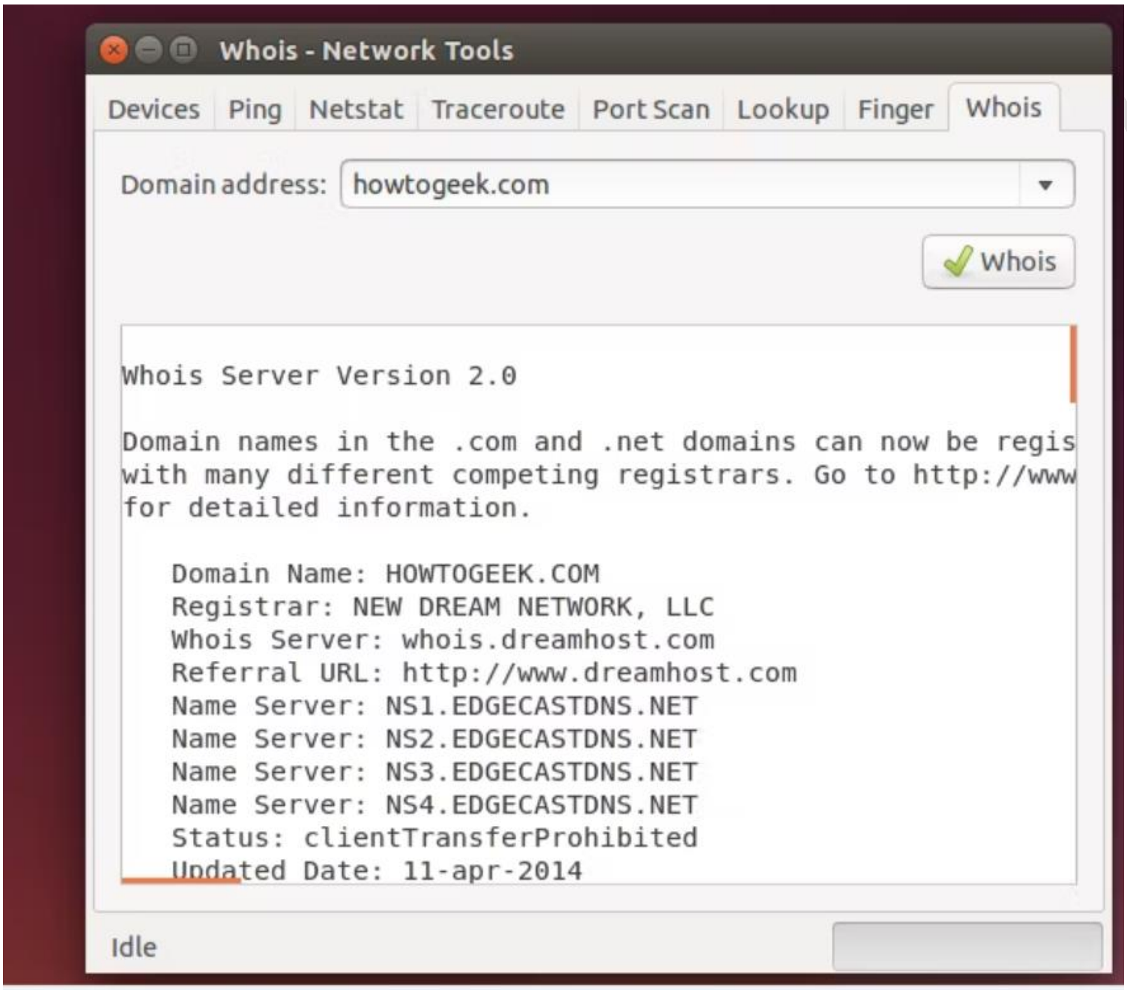
The whois command looks up the registration record associated with a domain name. This can show you more information about who registered and owns a domain name, including their contact information. Most modern versions of whois try to guess the right server to ask for the specified object. If no guess can be made, whois will connect to whois.networksolutions.com for NIC handles or whois.arin.net for IPv4 addresses and network names.

Examples:

- Obtaining the domain WHOIS record for computersolutions.com
- WHOIS record by IP querying
- Querying WHOIS in google search engine

WHOIS is a request and response protocol that follows the RFC 3912 specification. A WHOIS server listens on TCP port 43 for incoming requests. The domain registrar is responsible for maintaining the WHOIS records for the domain names it is leasing. The WHOIS server replies with various information related to the domain requested. Of particular interest, we can learn:

- Registrar: Via which registrar was the domain name registered?
- Contact info of registrant: Name, organization, address, phone, among other things. (unless made hidden via a privacy service)
- Creation, update, and expiration dates: When was the domain name first registered? When was it last updated? And when does it need to be renewed?
- Name Server: Which server to ask to resolve the domain name?



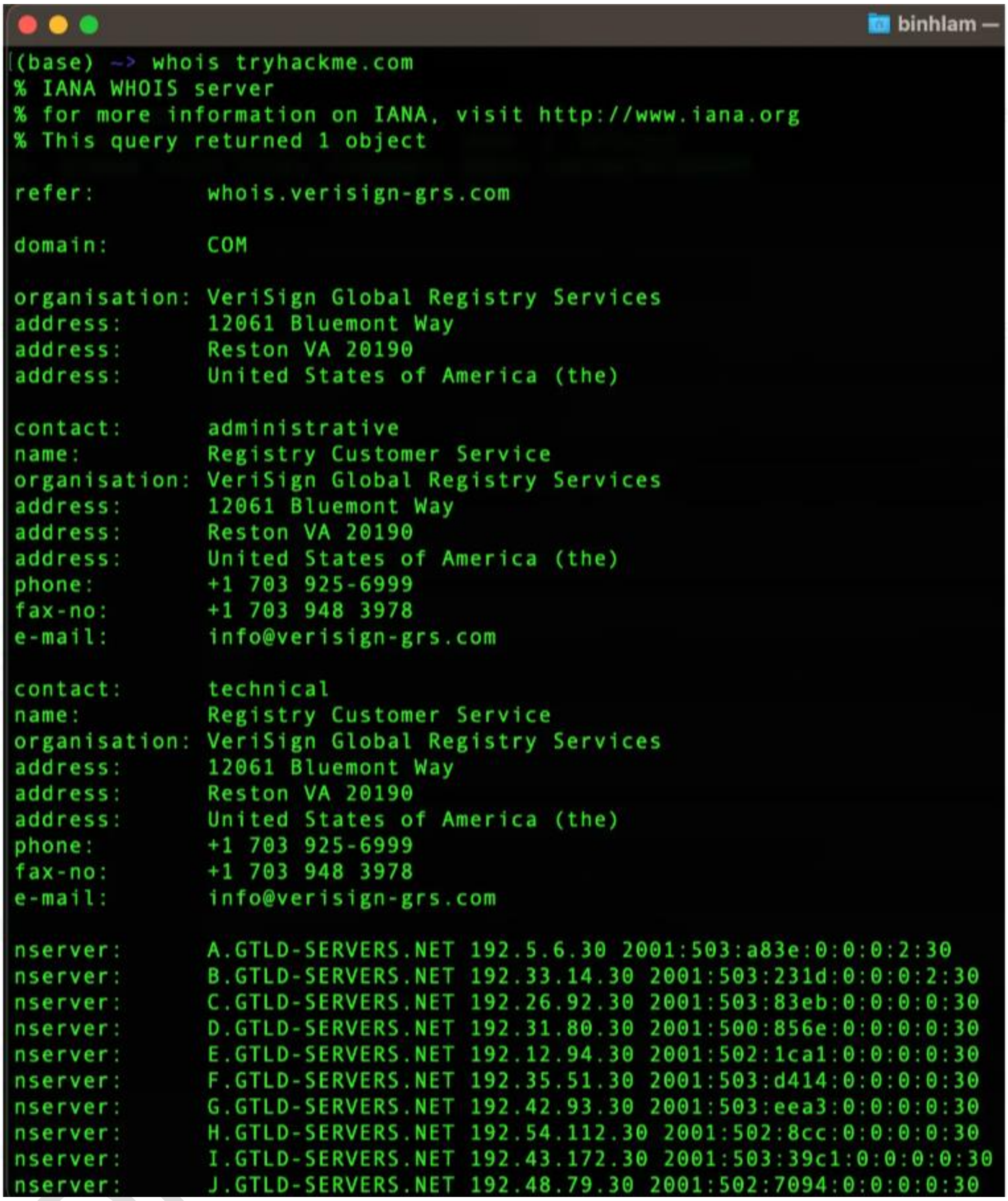
Domain address: howtogeek.com

```
Whois Server Version 2.0

Domain names in the .com and .net domains can now be regis
with many different competing registrars. Go to http://www
for detailed information.

   Domain Name: HOWTOGEEK.COM
   Registrar: NEW DREAM NETWORK, LLC
   Whois Server: whois.dreamhost.com
   Referral URL: http://www.dreamhost.com
   Name Server: NS1.EDGECASTDNS.NET
   Name Server: NS2.EDGECASTDNS.NET
   Name Server: NS3.EDGECASTDNS.NET
   Name Server: NS4.EDGECASTDNS.NET
   Status: clientTransferProhibited
   Updated Date: 11-apr-2014
```

Screenshot 1; WHOIS tool for gathering information related to howtogeek.com website.



```
binhlam —
(base) ~> whois tryhackme.com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.verisign-grs.com

domain:       COM

organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)

contact:      administrative
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

contact:      technical
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

nserver:      A.GTLD-SERVERS.NET 192.5.6.30 2001:503:a83e:0:0:0:2:30
nserver:      B.GTLD-SERVERS.NET 192.33.14.30 2001:503:231d:0:0:0:2:30
nserver:      C.GTLD-SERVERS.NET 192.26.92.30 2001:503:83eb:0:0:0:0:30
nserver:      D.GTLD-SERVERS.NET 192.31.80.30 2001:500:856e:0:0:0:0:30
nserver:      E.GTLD-SERVERS.NET 192.12.94.30 2001:502:1ca1:0:0:0:0:30
nserver:      F.GTLD-SERVERS.NET 192.35.51.30 2001:503:d414:0:0:0:0:30
nserver:      G.GTLD-SERVERS.NET 192.42.93.30 2001:503:eea3:0:0:0:0:30
nserver:      H.GTLD-SERVERS.NET 192.54.112.30 2001:502:8cc:0:0:0:0:30
nserver:      I.GTLD-SERVERS.NET 192.43.172.30 2001:503:39c1:0:0:0:0:30
nserver:      J.GTLD-SERVERS.NET 192.48.79.30 2001:502:7094:0:0:0:0:30
```

Screenshot 2; WHOIS tool for gathering information related to tryhackme.com

6.Conclusion: In this experiment you learned how to take the first steps toward ethical hacking. Information gathering, in the form of reconnaissance, foot printing, and social engineering, is necessary to learn as much about the target as possible. By following the information-gathering methodology, ethical hackers can ensure they are not missing any steps and valuable information. Time spent in the information- gathering phase is well worth it to speed up and produce successful hacking exploits.

Experiment 7: Show how to detect ARP Spoofing using open-source tool ARPWATCH.

1. Aim: Objective of the module to find ARP spoofing using open source.

2. Objectives: Detect ARP spoofing using open source tool ARPWATCH.

3. Hardware / Software Required: ARPWATCH Tool

4. Theory:

Arpwatch is a tool that monitors Ethernet activity on a network. It is designed to keep track of Ethernet/IP address pairings (ARP activity) and alert system administrator when any changes occur. ARP (Address Resolution Protocol) is a protocol used to map an IP address to a MAC address on a local network. Arpwatch is particularly useful for detecting potential network attacks such as ARP spoofing or MAC address spoofing, which can be used to intercept network traffic or launch a man-in-the-middle attack.

5. Methodology:

- **Installing Arpwatch**

Arpwatch can be installed on most Linux distributions using package manager. On Debian-based systems, you can install it using following command −

```
$ sudo apt-get install arpwatch
```

- **Configuring Arpwatch**

Once Arpwatch is installed, it needs to be configured before it can start monitoring network activity. configuration file for Arpwatch is located at /etc/arpwatch.conf.

Here is an example configuration file −

```
# arpwatch.conf
DEVICE=eth0
# Email address to send alerts to
#EMAIL_ADDRESS=root
eth0 -a -n 192.168.2.1/25
```

Next install syslog

```
sudo apt-get install rsyslog
```

Now enable arpwatch by using following command –

systemctl enable arpwatch@eth0

Then, start Arpwatch service using following command −

sudo service arpwatch start

Arpwatch will now begin monitoring Ethernet activity on specified network interface.

- Arpwatch Commands and Usage To watch a specific interface, type the following command with _-i_ and device name.

arpwatch -i eth0

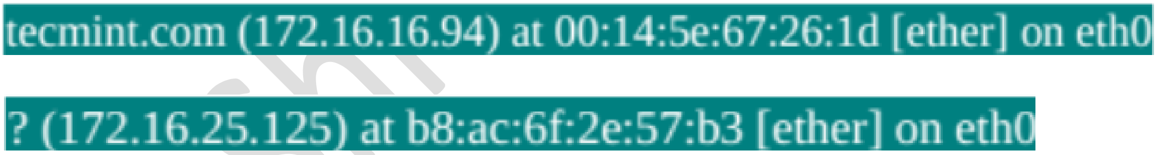
So, whenever a new MAC is plugged or a particular IP is changing his MAC address on the network, you will notice syslog entries at _/var/log/syslog_ or _/var/log/message_ file.

#tail -f/var/log/syslog

You can also check current ARP table, by using following command.

#arp -a

Sample Output:



```
tecmint.com (172.16.16.94) at 00:14:5e:67:26:1d [ether] on eth0

? (172.16.25.125) at b8:ac:6f:2e:57:b3 [ether] on eth0
```

ARP Spoofing (Man in Middle attack)

Use the following command to start ARP spoofing

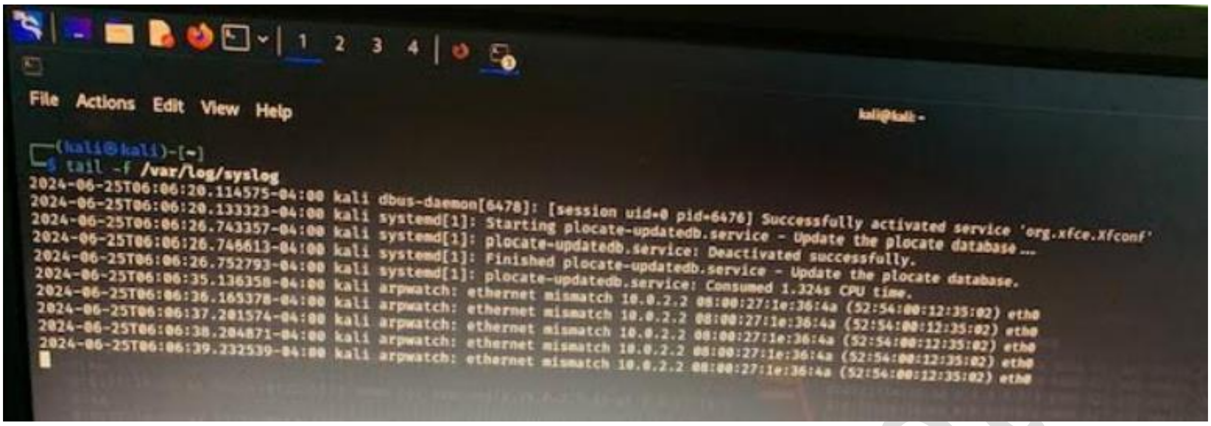
arpspoof -i eth0 -t 192.168.2.3 10.0.2.2

arpspoof -i eth0 -t 10.0.2.2 192.168.2.3

tail -f /var/log/syslog

Use separate terminals to execute these commands and Arpwatch must be enable and started.

The Arpwatch detects any changes in IP address and will be notified in the syslog messages. The syslog notify ethernet mismatch due to ARP spoofing.



```
┌──(kali㉿kali)-[~]
└─$ tail -f /var/log/syslog
2024-06-25T06:06:20.114575-04:00 kali dbus-daemon[6478]: [session uid=0 pid=6476] Successfully activated service 'org.xfce.Xfconf'
2024-06-25T06:06:20.133323-04:00 kali systemd[1]: Starting plocate-updatedb.service - Update the plocate database...
2024-06-25T06:06:26.743357-04:00 kali systemd[1]: plocate-updatedb.service: Deactivated successfully.
2024-06-25T06:06:26.746613-04:00 kali systemd[1]: Finished plocate-updatedb.service - Update the plocate database.
2024-06-25T06:06:26.752793-04:00 kali systemd[1]: plocate-updatedb.service: Consumed 1.324s CPU time.
2024-06-25T06:06:35.136358-04:00 kali arpwatch: ethernet mismatch 10.0.2.2 08:00:27:1e:36:4a (52:54:00:12:35:02) eth0
2024-06-25T06:06:36.165378-04:00 kali arpwatch: ethernet mismatch 10.0.2.2 08:00:27:1e:36:4a (52:54:00:12:35:02) eth0
2024-06-25T06:06:37.201574-04:00 kali arpwatch: ethernet mismatch 10.0.2.2 08:00:27:1e:36:4a (52:54:00:12:35:02) eth0
2024-06-25T06:06:38.204871-04:00 kali arpwatch: ethernet mismatch 10.0.2.2 08:00:27:1e:36:4a (52:54:00:12:35:02) eth0
2024-06-25T06:06:39.232539-04:00 kali arpwatch: ethernet mismatch 10.0.2.2 08:00:27:1e:36:4a (52:54:00:12:35:02) eth0
```

If you want to send alerts to your custom email id, then open the main configuration file_/etc/sysconfig/arpwatch_ and add the email as shown below.

```
# -u <username> : defines with what user id arpwatch should run

# -e <email>    : the <email> where to send the reports

# -s <from>     : the <from>-address

OPTIONS="-u arpwatch -e tecmint@tecmint.com -s 'root (Arpwatch)'"
```

6. Conclusion: Arpwatch is a software or program tool for monitoring Address Resolution Protocol traffic on a computer network. Its main goal is to detect arp poisoning attacks like (e.g. ARP Poisoning, Ettercap, and Netcut) also detect intruders in your network by sending an email to an administrator when new Ethernet MAC addresses seen on the network.

Experiment 8: Demonstrate network vulnerabilities by scanning network using Nessus tool.

1. Aim: Use the Nessus tool to scan the network for vulnerabilities.

2. Objectives: Objective of the module is scan system and network analysis.

3. Hardware / Software Required: Nessus Vulnerability Scanner | Tenable Network Security tool.

4. Theory:

Nessus is a proprietary comprehensive vulnerability scanner which is developed by Tenable Network Security. It is free of charge for personal use in a non-enterprise environment. Operation

- Nessus allows scans for the following types of vulnerabilities:
- Vulnerabilities that allow a remote hacker to control or access sensitive data on a system.
- Misconfiguration (e.g. open mail relay, missing patches, etc.).

Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.Denials of service against the TCP/IP stack by using malformed packets.

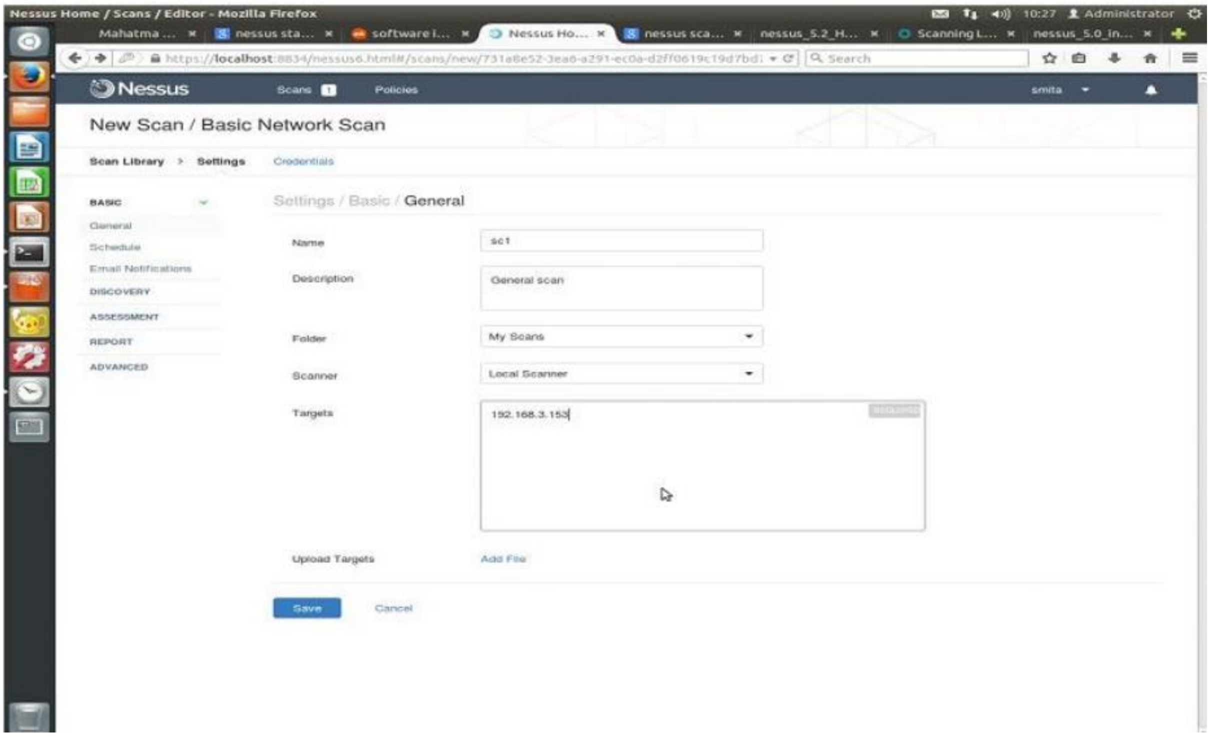
5. Methodology:

Preparation for PCI DSS audits

On UNIX (including Mac OS X), it consists of nessusd, the Nessus daemon, which does the scanning, and nessus, the client, which controls scans and presents the vulnerability results to the user. In typical operation, Nessus begins by doing a port scan with one of its four internal port scanners (or it can optionally use AmapM or Nmap) to determine which ports are open on the target and then tries various exploits on the open ports. The vulnerability tests, available as subscriptions, are written in NASL(Nessus Attack Scripting Language), a scripting language optimized for custom network interaction. Tenable Network Security produces several dozen new vulnerability checks (called plugins) each week, usually on a daily basis. These checks are available for free to the general public; commercial customers are not allowed to use this Home Feed any more. The Professional Feed (which is not free) also give access to support and additional scripts (e.g. audit files, compliance tests, additional vulnerability detection plugins).

Optionally, the results of the scan can be reported in various formats, such as plain text, XML, HTML and LaTeX. The results can also be saved in a knowledge base for debugging. On UNIX, scanning can be automated through the use of a command-line client. There exist many different commercial, free and open source tools for both UNIX and Windows to manage individual or distributed Nessus scanners. If the user chooses to do so (by disabling the option 'safe checks'), some of Nessus' vulnerability test may try to cause vulnerable services or operating systems to crash. This lets a user test the resistance of a device before putting it in production. Nessus provides additional functionality beyond testing for known network vulnerabilities. For instance, it can use Windows credentials to examine patch levels on computers running the Windows operating system, and can perform password auditing using dictionary and brute force methods. Nessus 3 and later can also audit systems to make sure they have been configured per a specific policy, such as the NSA's guide for hardening Windows servers.

Basic Network scanning:



Nessus Home / Scans / Editor - Mozilla Firefox

https://localhost:8834/nessus6.html#/scans/new/731a8e52-3ea8-a291-ec0a-d2ff0619c19d7bd

New Scan / Basic Network Scan

Scan Library > Settings   Credentials

Settings / Basic / General

Name: sc1

Description: General scan

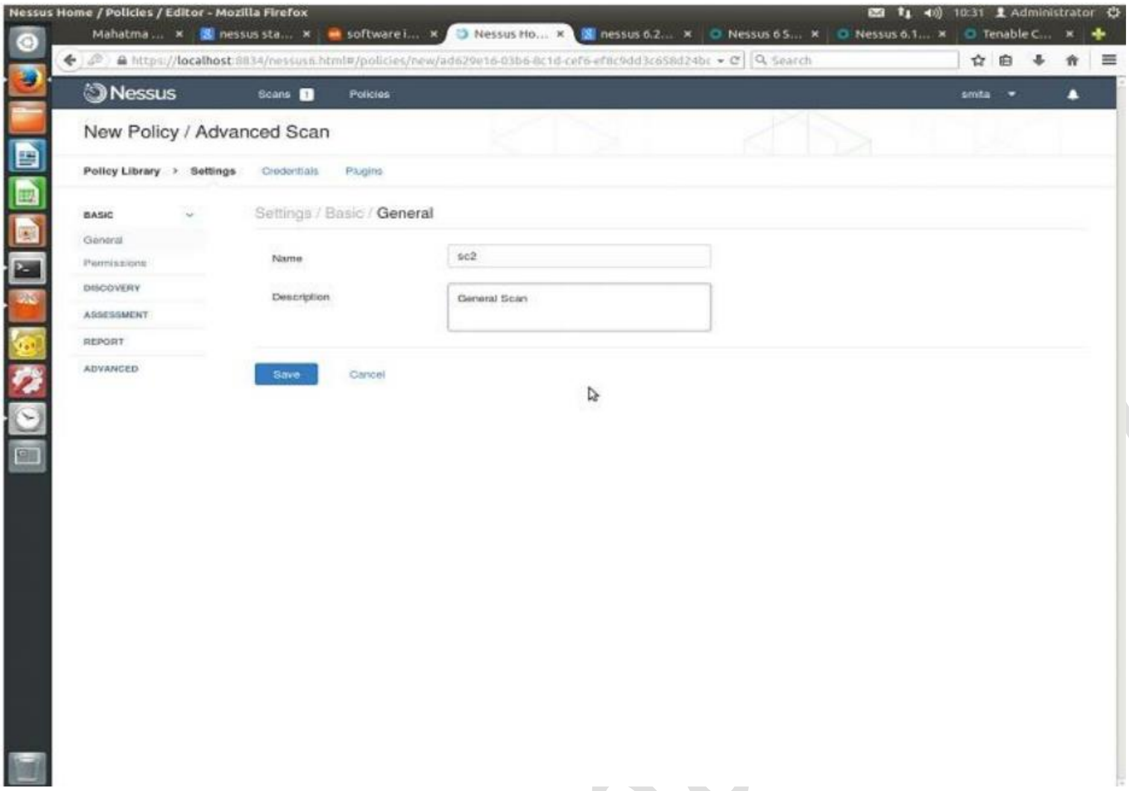
Folder: My Scans

Scanner: Local Scanner

Targets: 192.168.3.153

Upload Targets: Add File

Advanced scanning in general search:



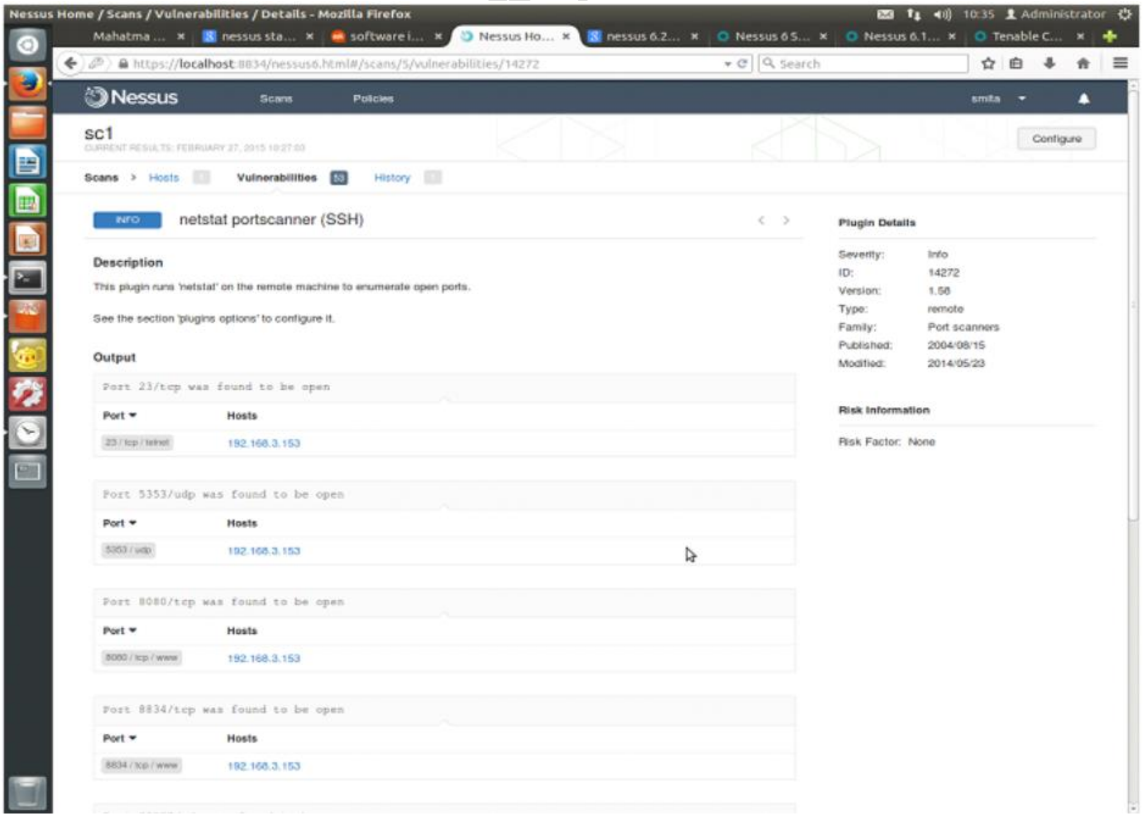
New Policy / Advanced Scan

Settings / Basic / General

Name: sc2

Description: General Scan

Ntstat port scanning:



sc1

CURRENT RESULTS: FEBRUARY 27, 2015 10:27:00

netstat portscanner (SSH)

Description

This plugin runs 'netstat' on the remote machine to enumerate open ports.

See the section 'plugins options' to configure it.

Output

```
Port 23/tcp was found to be open
```

Port	Hosts
23 / tcp / telnet	192.168.3.153

```
Port 5353/udp was found to be open
```

Port	Hosts
5353 / udp	192.168.3.153

```
Port 8080/tcp was found to be open
```

Port	Hosts
8080 / tcp / www	192.168.3.153

```
Port 8834/tcp was found to be open
```

Port	Hosts
8834 / tcp / www	192.168.3.153

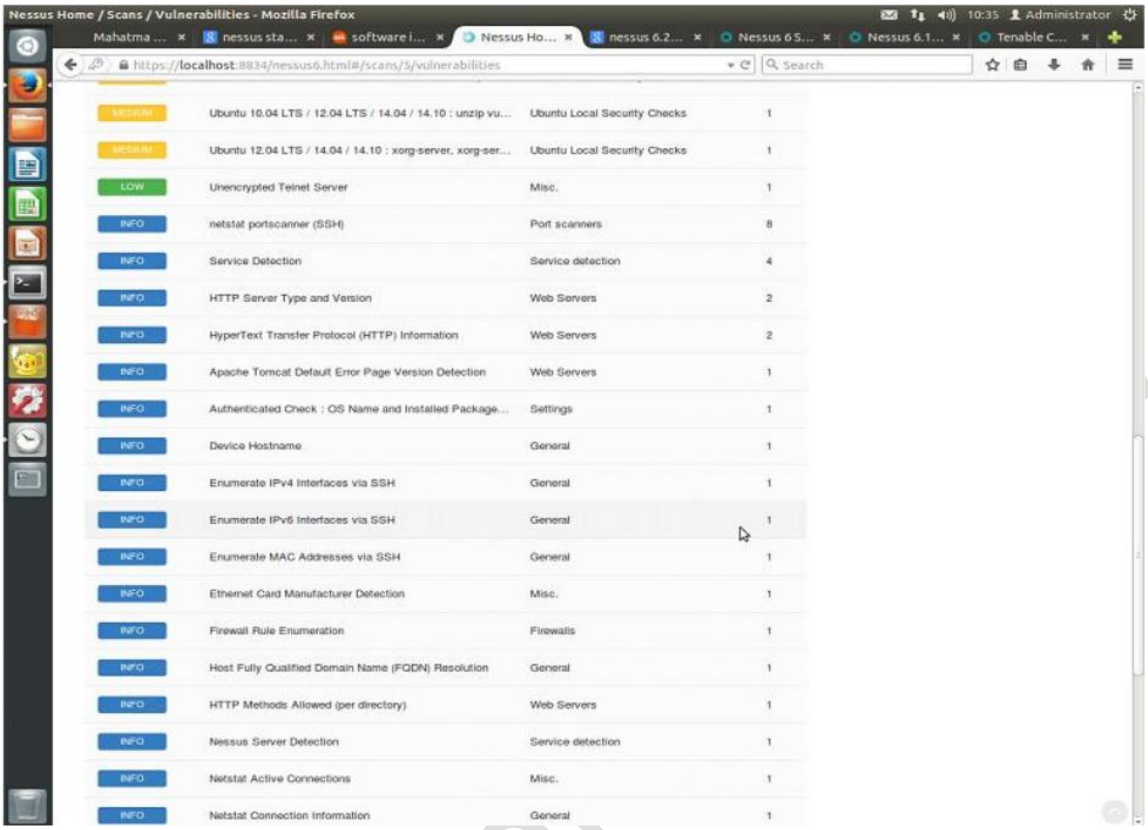
Plugin Details

Severity:	Info
ID:	14272
Version:	1.58
Type:	remote
Family:	Port scanners
Published:	2004/08/15
Modified:	2014/05/23

Risk Information

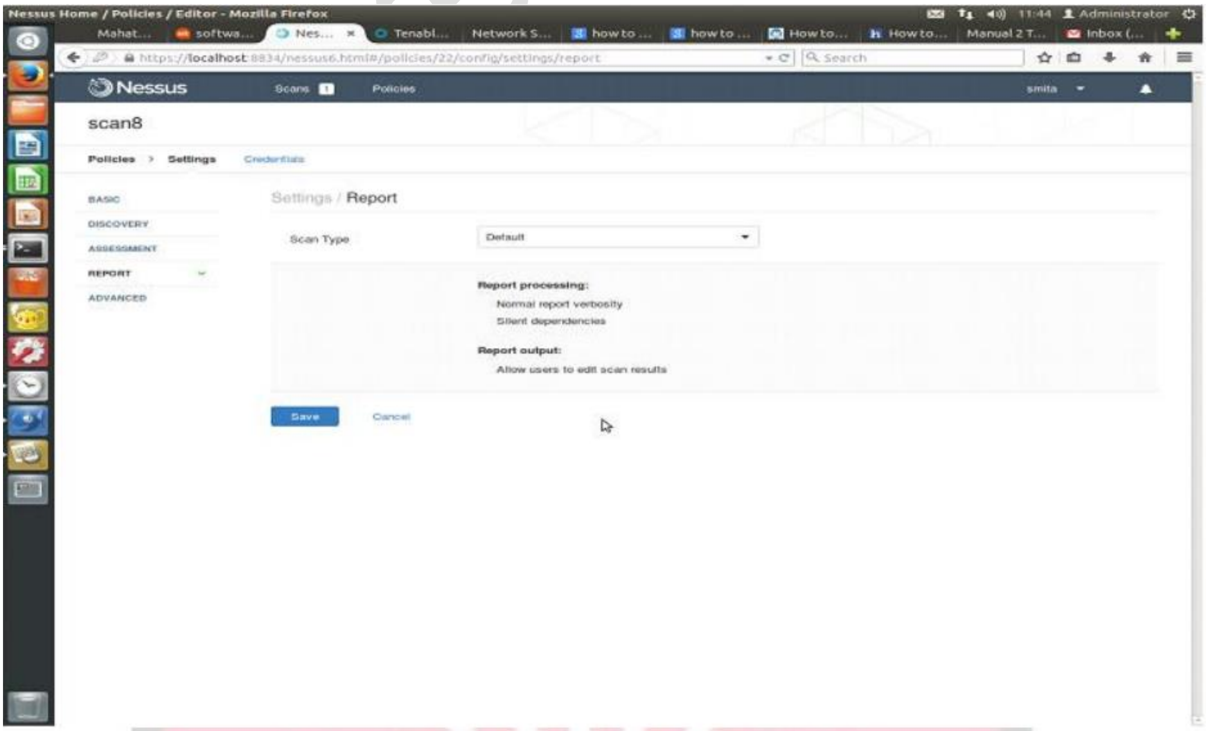
Risk Factor: None

Vulnerability Mapping:



MEDIUM	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : unzip vu...	Ubuntu Local Security Checks	1
MEDIUM	Ubuntu 12.04 LTS / 14.04 / 14.10 : xorg-server, xorg-ser...	Ubuntu Local Security Checks	1
LOW	Unencrypted Telnet Server	Misc.	1
INFO	netstat portscanner (SSH)	Port scanners	8
INFO	Service Detection	Service detection	4
INFO	HTTP Server Type and Version	Web Servers	2
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	2
INFO	Apache Tomcat Default Error Page Version Detection	Web Servers	1
INFO	Authenticated Check : OS Name and Installed Package...	Settings	1
INFO	Device Hostname	General	1
INFO	Enumerate IPv4 Interfaces via SSH	General	1
INFO	Enumerate IPv6 Interfaces via SSH	General	1
INFO	Enumerate MAC Addresses via SSH	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Firewall Rule Enumeration	Firewalls	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	HTTP Methods Allowed (per directory)	Web Servers	1
INFO	Nessus Server Detection	Service detection	1
INFO	Netstat Active Connections	Misc.	1
INFO	Netstat Connection Information	General	1

Policies:



scan8

Settings / Report

Scan Type: Default

Report processing:

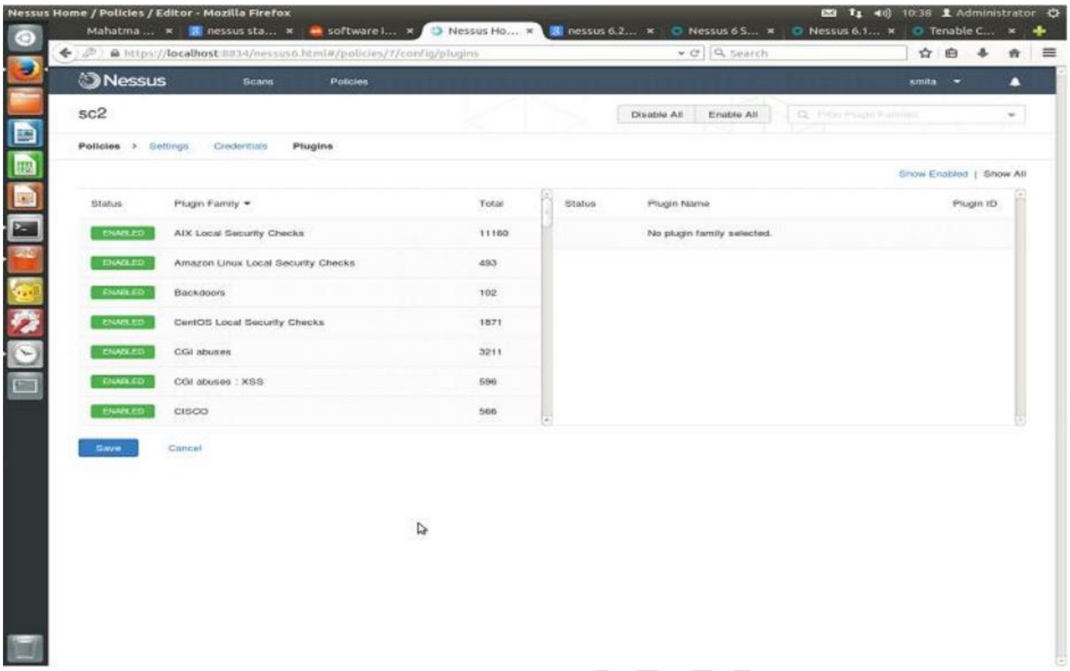
Normal report verbosity

Silent dependencies

Report output:

Allow users to edit scan results

Plugins:

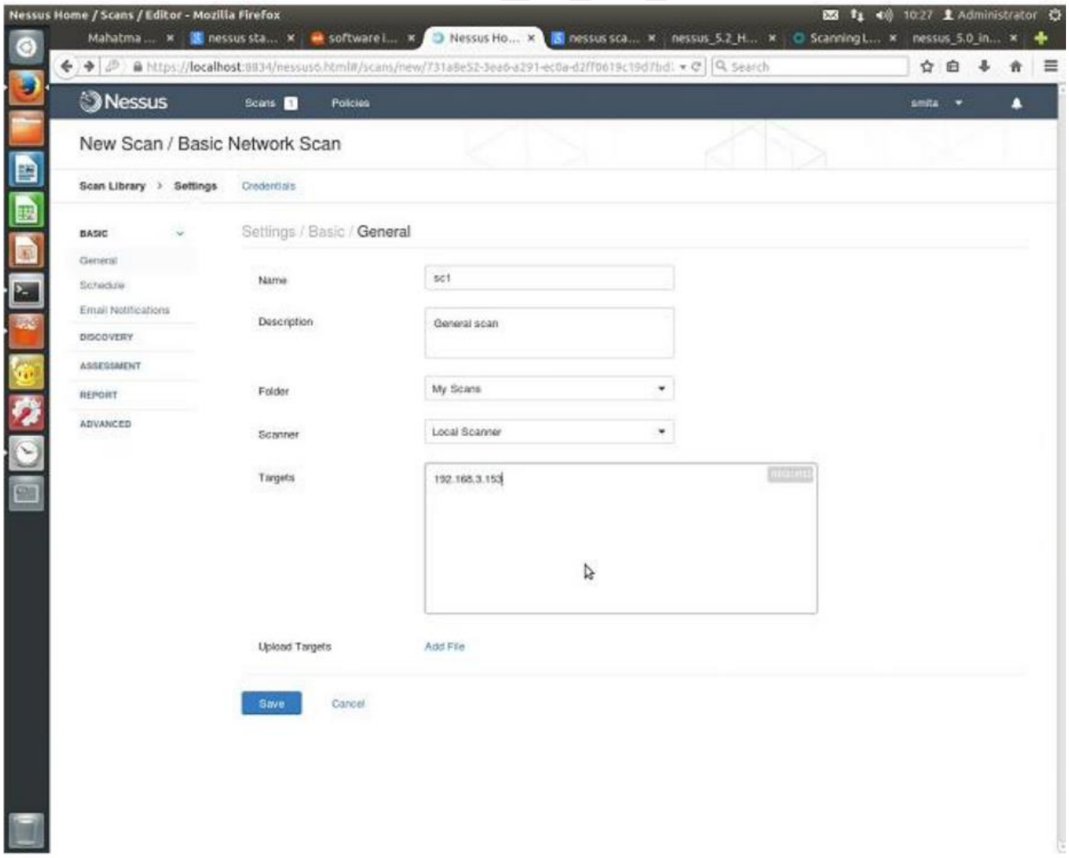


sc2

Status	Plugin Family ▾	Total
ENABLED	AIX Local Security Checks	11160
ENABLED	Amazon Linux Local Security Checks	493
ENABLED	Backdoors	102
ENABLED	CentOS Local Security Checks	1871
ENABLED	CGI abuses	3211
ENABLED	CGI abuses : XSS	596
ENABLED	CISCO	566

Status	Plugin Name	Plugin ID
	No plugin family selected.	

General Scanning:



New Scan / Basic Network Scan

Settings / Basic / General

Name: sc1

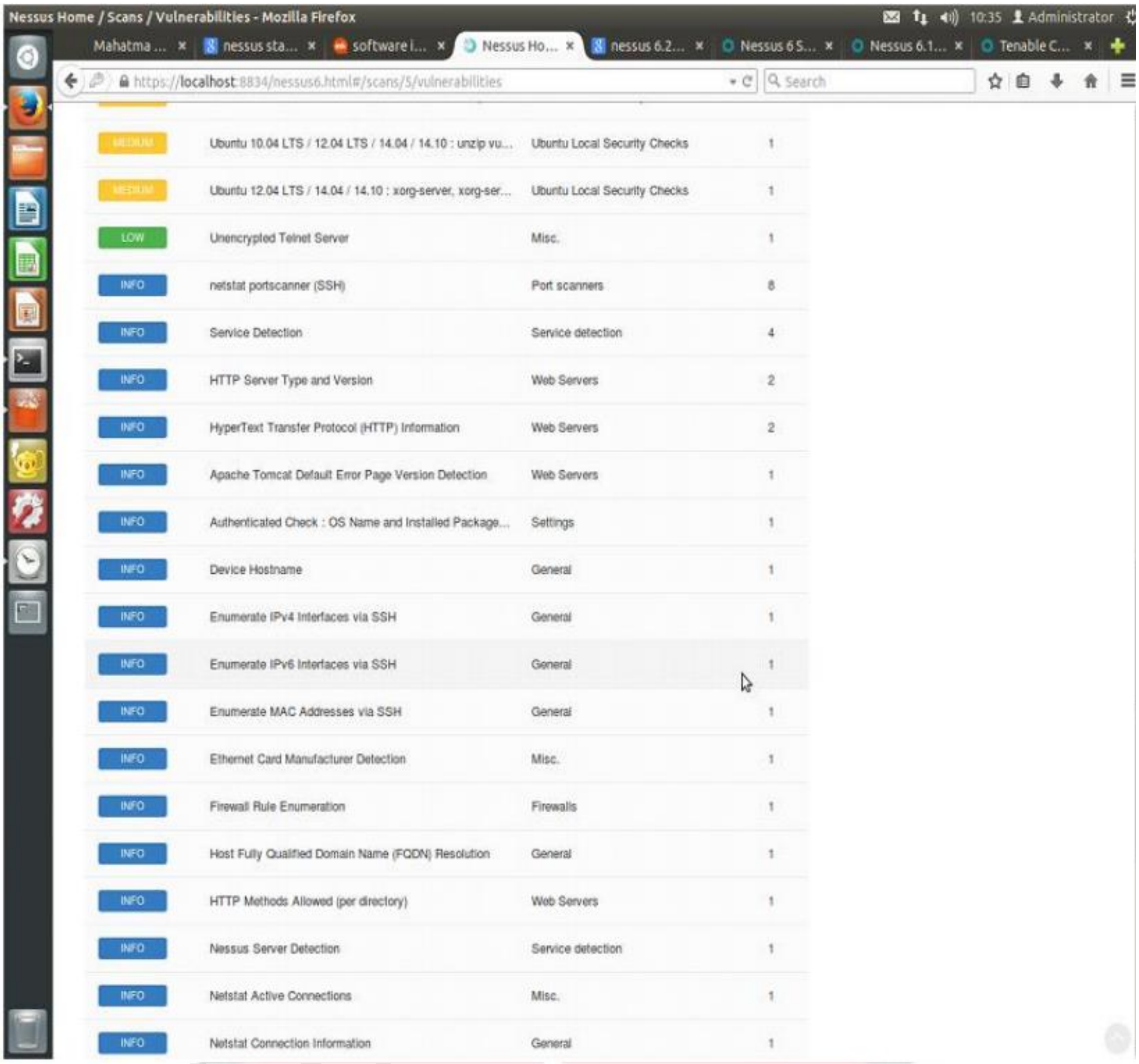
Description: General scan

Folder: My Scans

Scanner: Local Scanner

Targets: 192.168.3.153

Port Scanning:



MEDIUM	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : unzip vu...	Ubuntu Local Security Checks	1
MEDIUM	Ubuntu 12.04 LTS / 14.04 / 14.10 : xorg-server, xorg-ser...	Ubuntu Local Security Checks	1
LOW	Unencrypted Telnet Server	Misc.	1
INFO	netstat portscanner (SSH)	Port scanners	8
INFO	Service Detection	Service detection	4
INFO	HTTP Server Type and Version	Web Servers	2
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	2
INFO	Apache Tomcat Default Error Page Version Detection	Web Servers	1
INFO	Authenticated Check : OS Name and Installed Package...	Settings	1
INFO	Device Hostname	General	1
INFO	Enumerate IPv4 Interfaces via SSH	General	1
INFO	Enumerate IPv6 Interfaces via SSH	General	1
INFO	Enumerate MAC Addresses via SSH	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Firewall Rule Enumeration	Firewalls	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	HTTP Methods Allowed (per directory)	Web Servers	1
INFO	Nessus Server Detection	Service detection	1
INFO	Netstat Active Connections	Misc.	1
INFO	Netstat Connection Information	General	1

6. Conclusion:

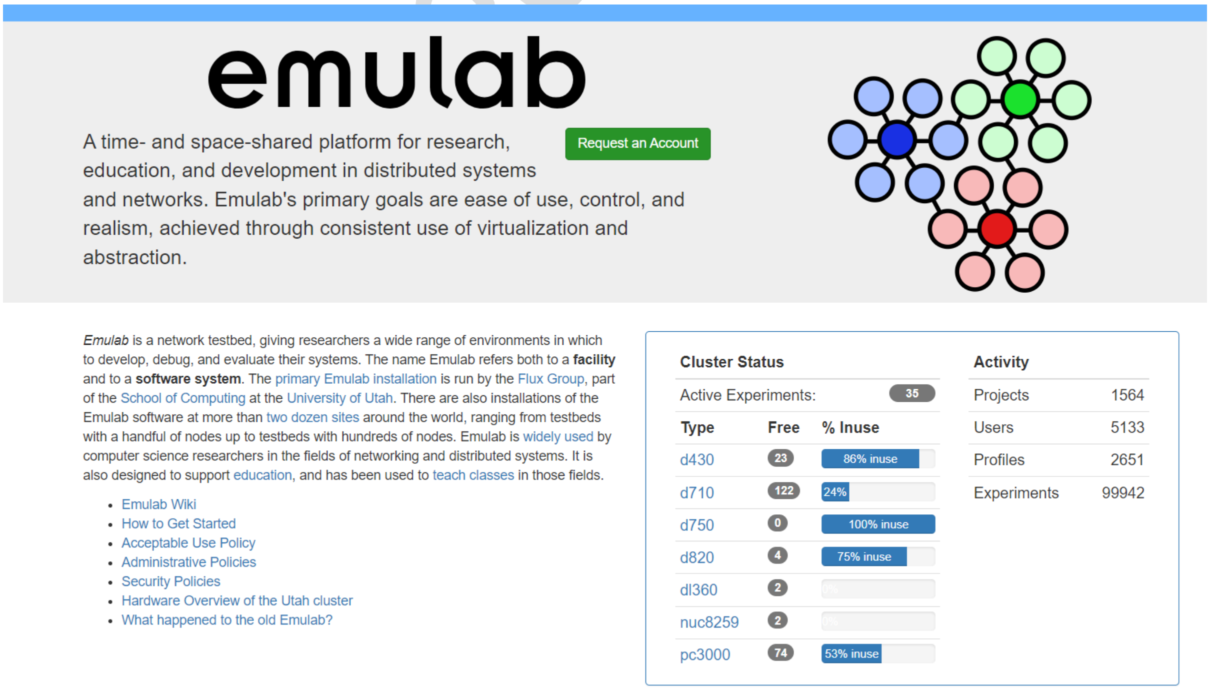
Running a security scanner against your systems is a very important part of the job. It is a system administrator or security officer‘s job to keep their systems secure and the data contained in them safe. Hackers have access to all the same information and tools that the rest of us do. Hackers run the very same tools and it is advantageous to know what the results are that they see if they scan your system. They find time to do the research, so we must also. Nessus provides a lot of functionality in one tool. It utilizes Nmap, easy to update plug-ins, and nice reporting tools for upper management. It is has repeatedly scored high on comparisons between scanners including commercial scanners that come with a hefty price tag. And of course as budgets tighten, remember Nessus is a free tool. The only cost is the users time in learning it and using it, but that is a cost associated with all tools. Nessus is an easy to learn tool. Using this tool and seeing the vulnerabilities will help you gain knowledge of your systems and help teach you how to protect them.

Experiment 9: Demonstrate network testbed Emulab.

1. **Aim**: Demonstrate and understand network testbed Emulab.
2. **Objectives:** Understanding Emu test bed setup.
3. **Hardware / Software Required:** Emulab Test bed.
4. **Theory:**

Emulab is a testbed that has been developed at the University of Utah since 1999. Emulab can provide unlimited experimental environments in which researchers can develop, debug and evaluate their systems. Emulab is also designed for education. Emulab can coordinate a composite system that includes numerous physical computers as nodes. Each computer has six network interface cards. The first network interface card manages user logins, power on signals, power off signals, and other control signals. The other five network interface cards are connected to a hardware switch. Emulab can manage various virtual local area networks (VLANs) and connect one or more VLANs to each computer in this system. Each user navigates to a web interface to request the resources or access the topology of the network. Emulab allocates all resources within this system.

5. **Get Started with Emu lab Test bed.**



A time- and space-shared platform for research, education, and development in distributed systems and networks. Emulab's primary goals are ease of use, control, and realism, achieved through consistent use of virtualization and abstraction.

Emulab is a network testbed, giving researchers a wide range of environments in which to develop, debug, and evaluate their systems. The name Emulab refers both to a **facility** and to a **software system**. The primary Emulab installation is run by the Flux Group, part of the School of Computing at the University of Utah. There are also installations of the Emulab software at more than two dozen sites around the world, ranging from testbeds with a handful of nodes up to testbeds with hundreds of nodes. Emulab is widely used by computer science researchers in the fields of networking and distributed systems. It is also designed to support education, and has been used to teach classes in those fields.

- Emulab Wiki
- How to Get Started
- Acceptable Use Policy
- Administrative Policies
- Security Policies
- Hardware Overview of the Utah cluster
- What happened to the old Emulab?

Cluster Status

Active Experiments: 35

Type	Free	% Inuse
d430	23	86% inuse
d710	122	24%
d750	0	100% inuse
d820	4	75% inuse
dl360	2	0%
nuc8259	2	0%
pc3000	74	53% inuse

Activity

Projects	1564
Users	5133
Profiles	2651
Experiments	99942

5.1 Configuring Emulab

An Emulab testbed is easily configured to support operational exercises. This section describes the steps involved in the design, setup, execution and analysis phases.

1. **Design Phase**
   After determining the participants and developing a detailed scenario, the following tasks are performed:The network topology is described using an experiment script. The components (e.g., servers and routers) to be controlled by the participants are differentiated from the components that simulate the rest of the world (i.e., the context). The exercise monitoring infrastructure is described and the data collection mechanisms are configured.
2. **Setup Phase**
   In the setup phase, the predefined systems are instantiated and configured as in any Emulab experiment. Exercise participants are given access to individual experimental nodes. Access control mechanisms are used to ensure that participants may only access the nodes "owned" by them in the scenario. However, exercise moderators are permitted to access all resources.
3. **Execution Phase**
   During the exercise execution phase, the participants interact with the systems and among themselves. Their actions are monitored for further analysis after the end of the exercise (analysis phase). It is important that exercise moderators know how the exercise is evolving so that they can intervene (e.g., by injecting dynamic events) if necessary.
4. **Analysis Phase**
   In the analysis phase, the emulation testbed is used to gather recorded data. The data is used to evaluate the response times, durations of actions, levels of coordination, etc. The data collected depends on the scope of the exercise.

   Example exercise setup Demo in Emulab

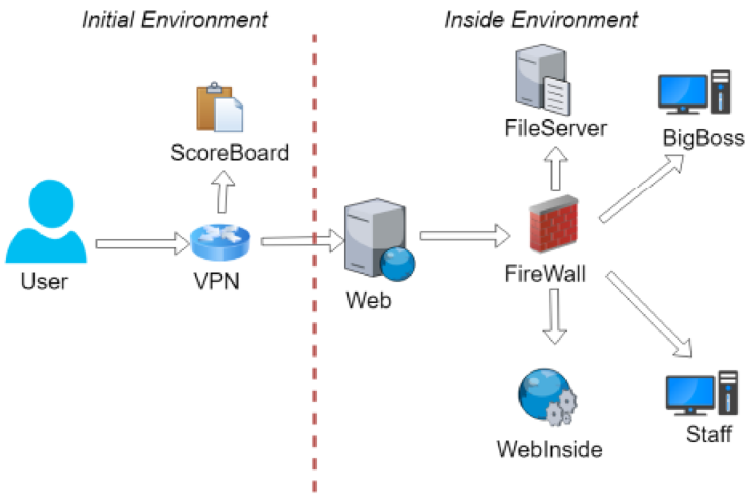
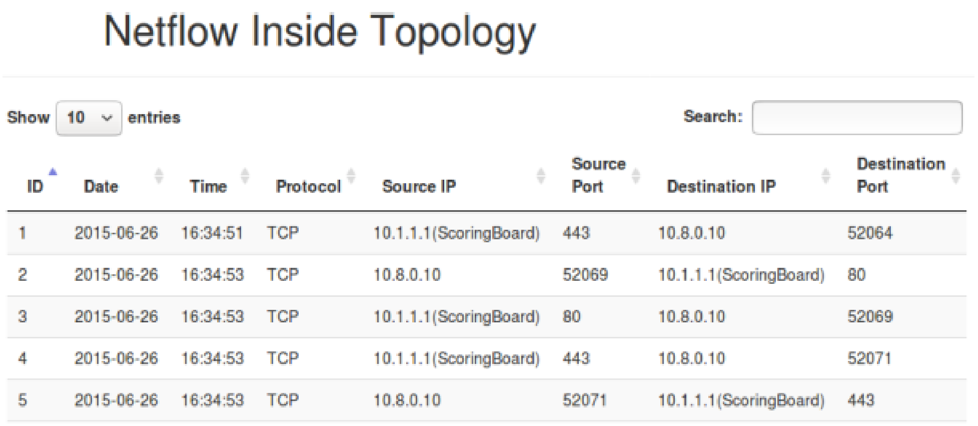


FIGURE 1. The topology of the scenario

The topology and related processes of the attack and defense scenario were as shown in Figure 1. In the experiment, a fixed cybersecurity attack and defense scenario was used in an environment designed for a three-party network.

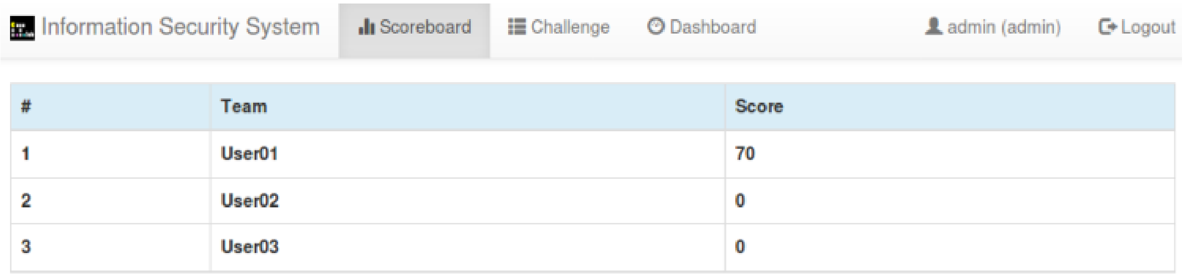


Netflow Inside Topology

ID	Date	Time	Protocol	Source IP	Source Port	Destination IP	Destination Port
1	2015-06-26	16:34:51	TCP	10.1.1.1(ScoringBoard)	443	10.8.0.10	52064
2	2015-06-26	16:34:53	TCP	10.8.0.10	52069	10.1.1.1(ScoringBoard)	80
3	2015-06-26	16:34:53	TCP	10.1.1.1(ScoringBoard)	80	10.8.0.10	52069
4	2015-06-26	16:34:53	TCP	10.1.1.1(ScoringBoard)	443	10.8.0.10	52071
5	2015-06-26	16:34:53	TCP	10.8.0.10	52071	10.1.1.1(ScoringBoard)	443

FIGURE 2. Netflow Inside Topology interface

During the test, participant traffic is directed to the topology through a virtual private network; the real traffic of the participants is recorded by Netflow Inside Topology (Figure 2). As shown in Figure 3, the scoreboard displays the current scores of the participants (teams).



#	Team	Score
1	User01	70
2	User02	0
3	User03	0

FIGURE 3. Appearance of scoreboard

6.Conclusion

A platform based on Emulab was demonstrated. This platform was dedicated to training and experience exchange. The cybersecurity attack and defense exercises provided through this platform trained the participants regarding the methods, techniques, and mechanisms used in attack and defense maneuvers.

10. Study of Information Technology Act, 2000 (India)

AMENDMENTS IN IT ACT 2000

The Information Technology Act was enacted in the year 2000 to bring in the necessary changes for growth of digitalisation and e-commerce transactions, and ensure safety and security of such transactions, thereby preventing crimes. The act was then amended to account for the developments in the domain, these amendments were passed by both the houses of Parliament in 2008 and received President's assent on 5th February, 2009, thus becoming the Amendment Act. It introduced various positive developments. It was seen as an effort by the Government of India to create a policy that is able to maintain pace with the evolving technology. The Indian Computer Emergency Response Team (CERT-In) is responsible for administration of the Act. The amendment attempted to fill in the gaps left by the earlier Act, and address the security concerns. The Act was the need of the hour as with increasing digitalisation, the crimes in the digital space or with the help of digital aids also proliferated. Sending/sharing offensive content, phishing, identity theft, frauds, etc. were crimes which had to be brought within the ambit of penal provisions. All these factors led to the amendments in IT Act 2000, thus paving the way for IT Act 2008. The IT Act 2008 revolutionized the cyber law framework of the nation. The Act addressed various issues such as incorporating electronic signature, inclusion of greater number of cyber offences, addressing the concerns pertaining to data protection, privacy, and also dealt with the issues related to use of digital/cyber medium for terrorism.

The features of The IT Act, 2000 are as follows:

1. The digital signature has been changed to an electronic signature to make it a greater generation-impartial act.
2. It elaborates on offenses, penalties, and breaches.
3. It outlines the Justice Dispensation Systems for cybercrimes.
4. The Information Technology Act defines in a new segment that a cyber cafe is any facility wherein access to the net is offered by any person inside the normal business to the general public.
5. It offers the constitution of the Cyber Regulations Advisory Committee.

6. The Information Technology Act is based totally on The Indian Penal Code, of 1860, The Indian Evidence Act, of 1872, The Bankers' Books Evidence Act, of 1891, The Reserve Bank of India Act, of 1934, and many others.
7. It adds a provision to Section 81, which states that the provisions of the Act shall have overriding effect. The provision states that nothing contained inside the Act shall limit any person from exercising any right conferred under the Copyright Act, of 1957.

The Offenses and the Punishments in IT Act 2000

The offenses and the punishments that fall under the IT Act, of 2000 are as follows: -

1. Tampering with the computer source documents.
2. Directions of Controller to a subscriber to extend facilities to decrypt information.
3. Publishing of information that is obscene in electronic form.
4. Penalty for breach of confidentiality and privacy.
5. Hacking for malicious purposes.
6. Penalty for publishing Digital Signature Certificate false in certain particulars.
7. Penalty for misrepresentation.
8. Confiscation.
9. Power to investigate offenses.
10. Protected System.
11. Penalties for confiscation are not to interfere with other punishments.
12. Act to apply for offense or contravention committed outside India.
13. Publication for fraud purposes.
14. Power of Controller to give directions.

Conclusion

It is an act to show misconduct behavior for transactions executed by way of electronic information interchange and another approach of electronic conversation, usually referred to as “electronic commerce”, which contains the usage of alternatives to paper-based methods of communication and storage of information, to facilitate digital submission of documents with the Government agencies.