NETWORK INTRUSION, DETECTION AND PREVENTION SYSTEM

PREPARED FOR

Network Information and Security(ITE4001)

SUBMITTED TO

PROF. MANIVANNAN SIR

PREPARED BY

HARSH GUPTA	**15BIT0341**
SOURABH AGRAWAL	**15BIT0298**
SAHAJ MAHESHWARI	**15BIT0097**

B.Tech. IT – Winter 2017-2018

School of Information Technology and Engineering

Problem Statement:

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. While anomaly detection and reporting are the primary function, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses.

Existing System Drawbacks:

Factors like noise in the audit data, constantly changing traffic profiles, and the large amount of network traffic make it difficult to build a normal traffic profile of a network for the purpose of intrusion detection.

The implication is that, short of some fundamental redesign, today's intrusion detection approaches will not be able to adequately protect tomorrow's networks against intrusions and attacks. Therefore, the design methodology of intrusion detection systems needs to closely follow the changes in system and networking technologies.

Proposed System Architecture:

Our system provide a secure service where user can login and keep his important files secured.

Our system is a 3 Layer security system:

layer 1:

Usually the password is getting stored in the database as it is, so attackers can do sql injection attack and get the password of the user from the database easily. So, in the layer 1 we are encrypting the user's password by MD5 encryption algorithm and then storing the password in the database.

Layer 2:

Suppose no attacker attacks on our system with sql injection attack then what he gets is encrypted password. We designed a tool by

which hacker can decrypt the MD5 encrypted password by using Burte Force Attack.

Here we are limiting the password to 1-10,000(4 digit pin) because we are performing the decryption in the browser but limit can be increased.

So, by using the tool suppose attacker successfully decrypted the password. So, now he has both username and the password but still he can not penetrate the system. Here comes our layer 3 security.

Layer 3:

In the previous step attacker successfully got the username and the password.

But still he will not be able to log into our system because we are storing the “IP details”, user’s browser details(browser name, browser version, operating system) in our database.

So, if some unknown person try to logs in then an alert will be send to the original user that “Your account is attacked”.

Background Theory:

Intrusion Detection Systems are also as important as the firewall because they help us to detect the type of attack that is being done to our system and then to make a solution to block them. The monitoring part like tracing logs, looking for doubtful signatures and keeping history of the events triggered. They help also the network administrators to check the connection integrity and authenticity that occur.

MD5:

As MD5 hash generates the same encrypted value for the same password every time, it is better to send the Salted MD5 hash value of the password. The following tutorial explains about how to use Salted MD5 Hash for securing login passwords.

```
<?php
  $str = "any text";
```

```
  echo md5($str);
?>
```

Intrusion detection by host:

Are usually installed on servers and are more focused on analyzing the specific operating systems and applications, resource utilization and other system activity residing on the Host-based IDS host.

It will log any activities it discovers to a secure database and check to see whether the events match any malicious event record listed in the knowledge base.

Host Based Intrusion Detection

Host-based IDS are often critical in detecting internal attacks directed towards an organization’s servers such as DNS, Mail, and Web Servers

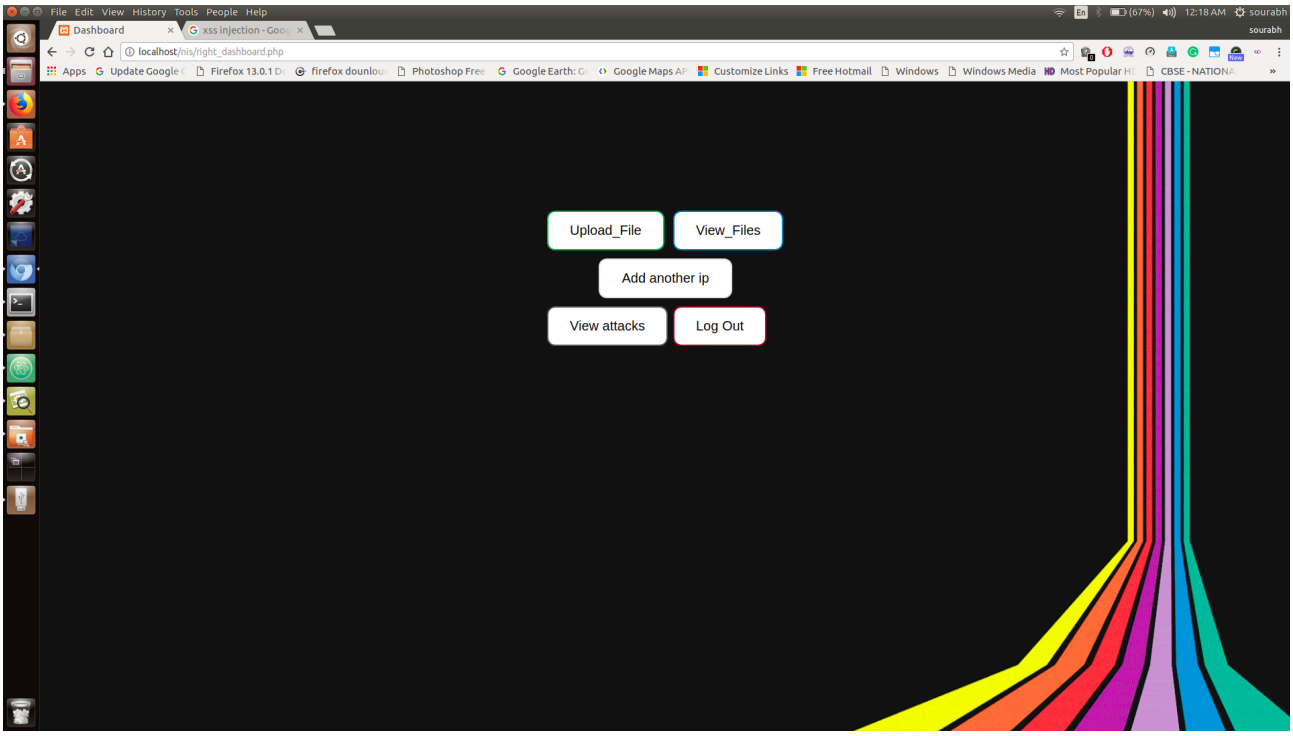
Are usually installed on servers and are more focused on analyzing the specific operating systems and applications, resource utilization and other system activity residing on the Host-based IDS host.

}It will log any activities it discovers to a secure database and check to see whether the events match any malicious event record listed in the knowledge base.

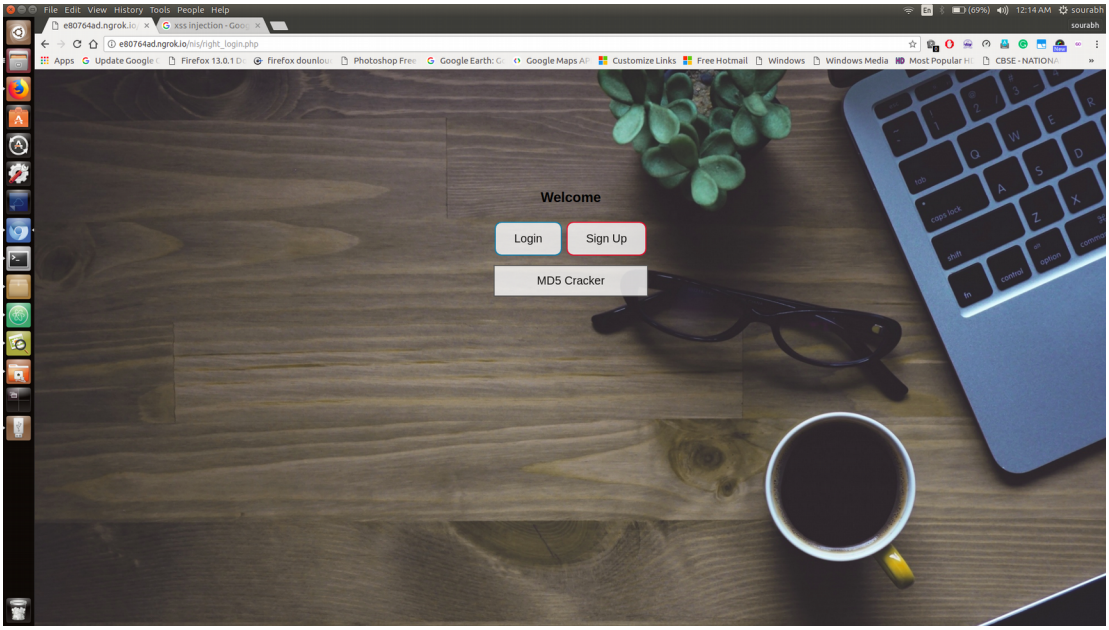
Host-based IDS are often critical in detecting internal attacks directed towards an organization’s servers such as DNS, Mail, and Web Servers.

SCREENSHOTS/ GLIMPSE OF PROJECT

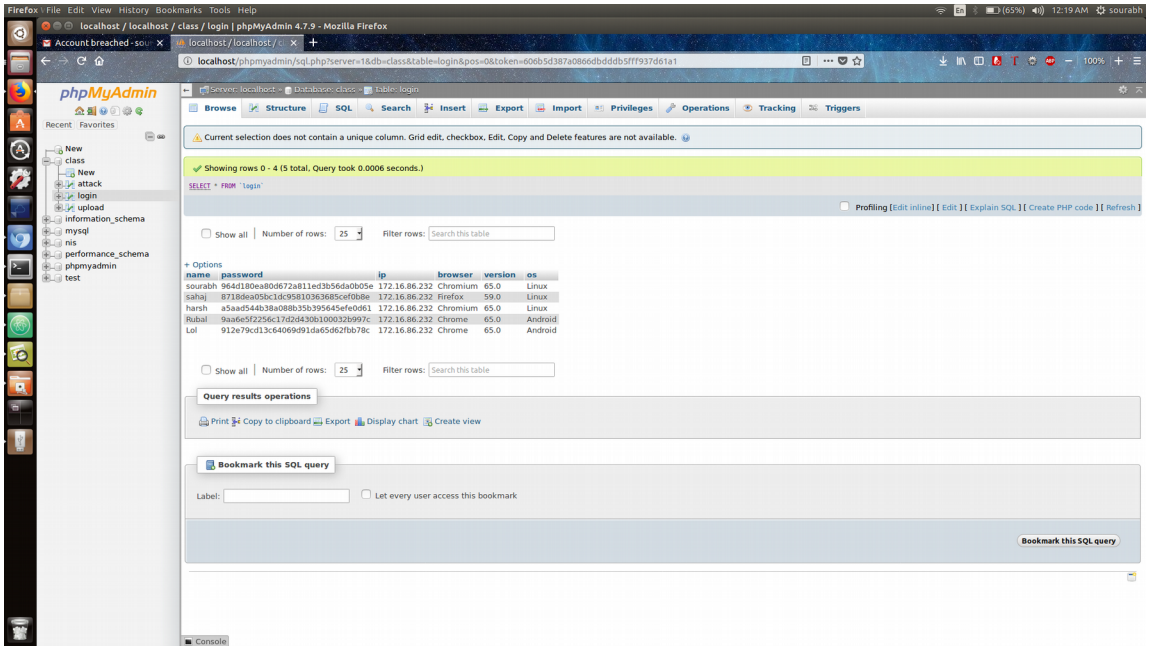
DASHBOARD



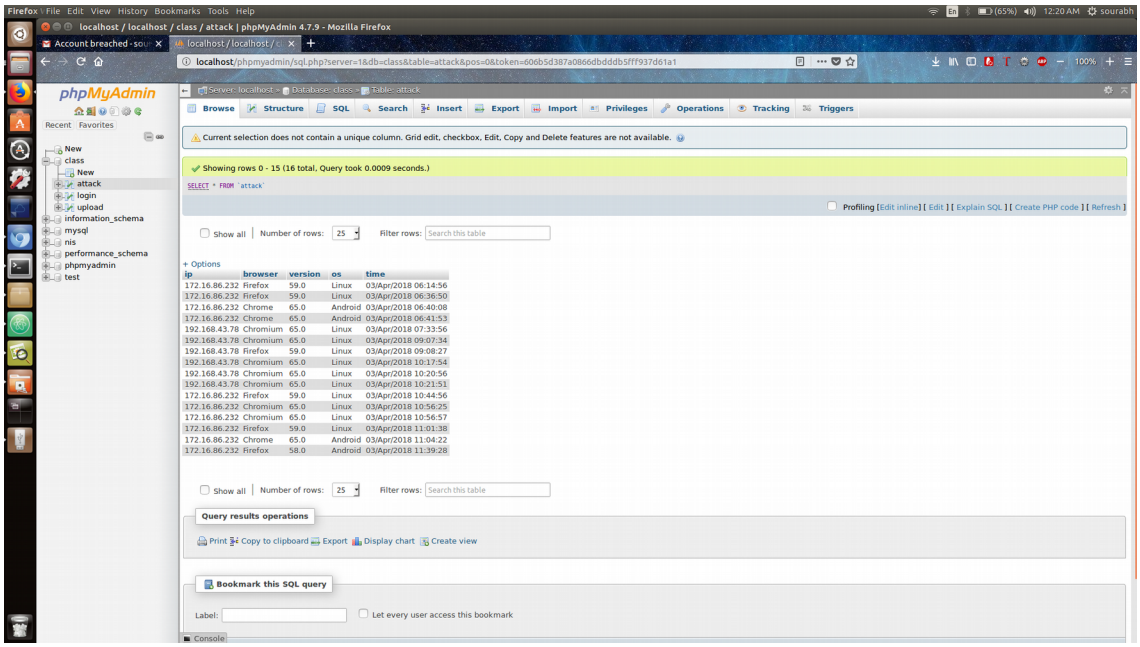
HOME PAGE:



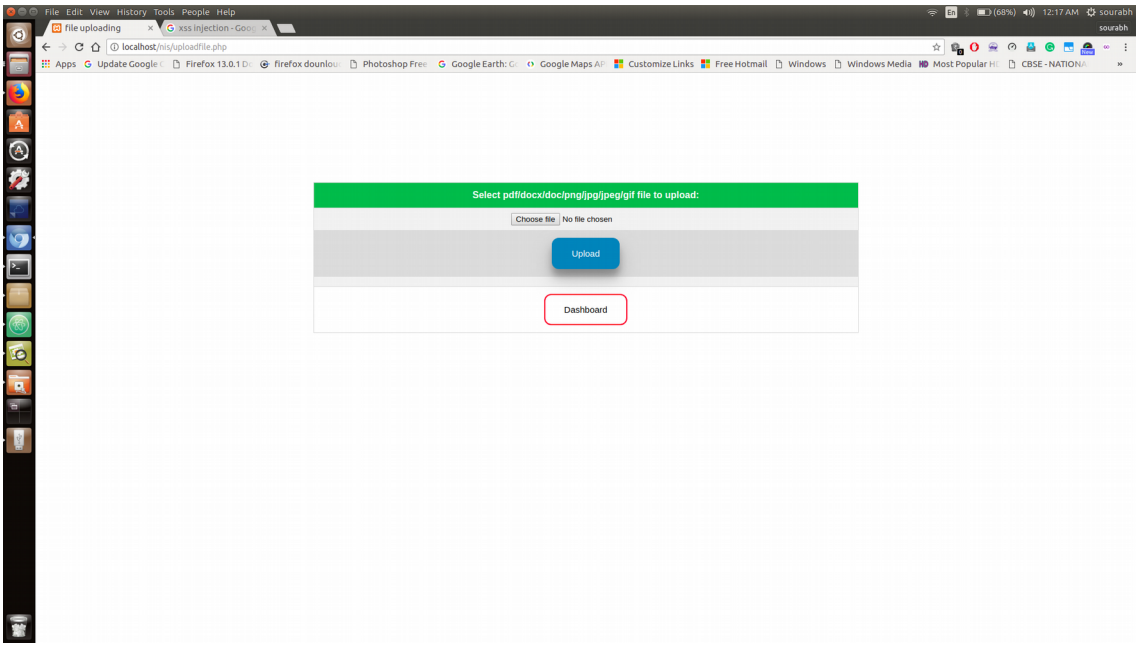
SAVED LOGIN IN DATABASE:



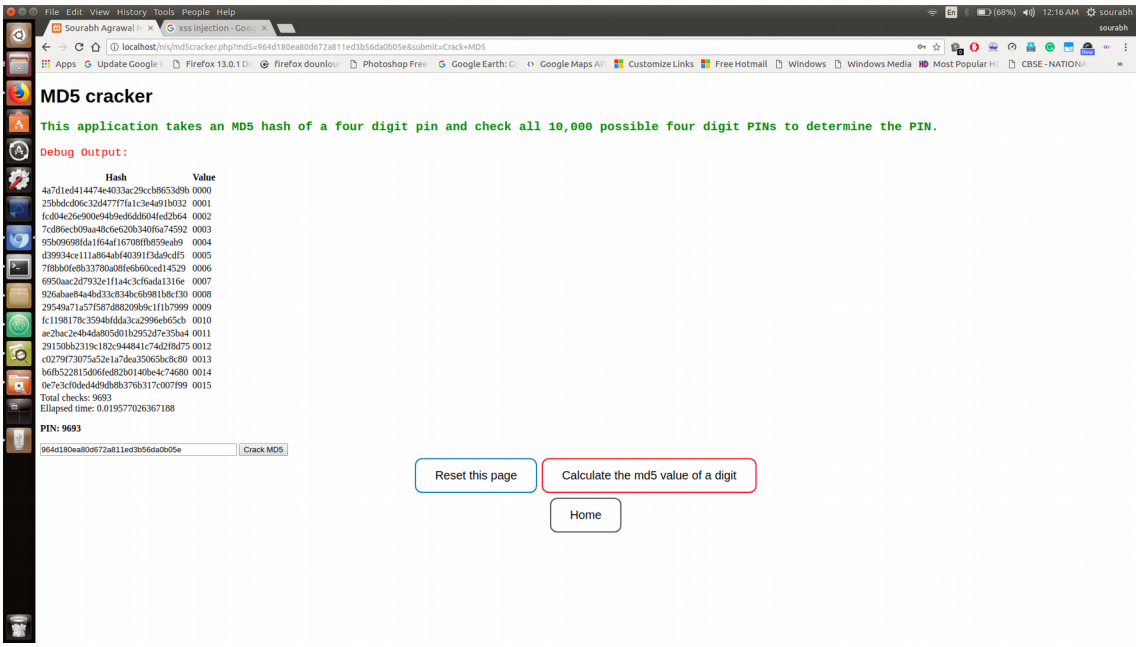
ATTACKERS INFORMATION STORED IN THE DATABASE:



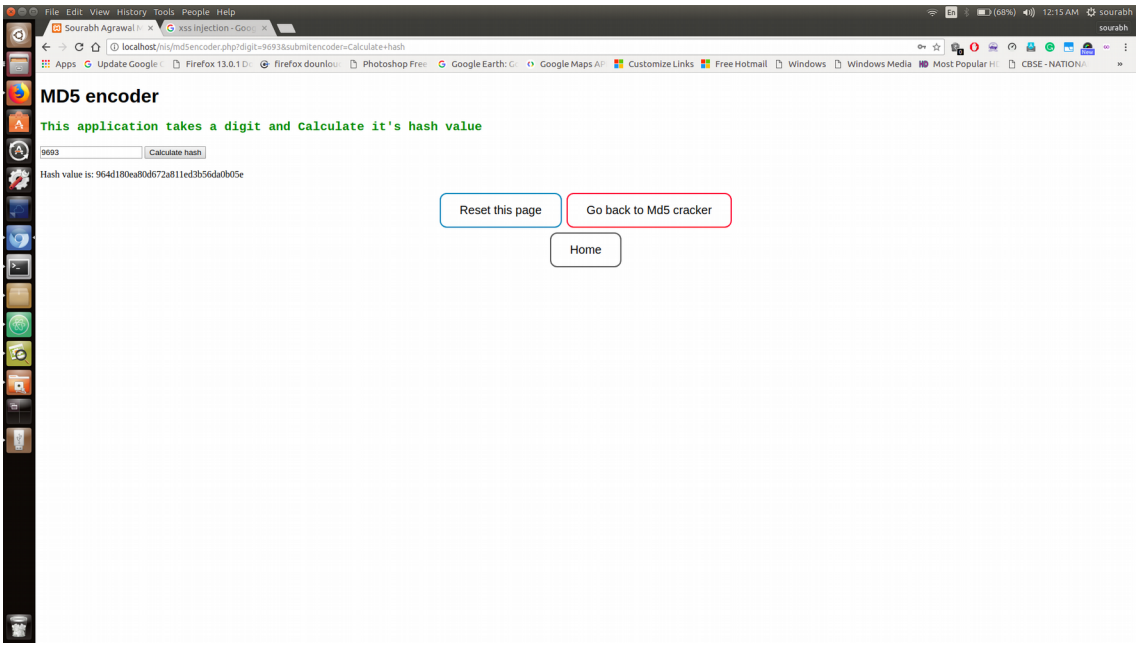
FILE UPLOADING



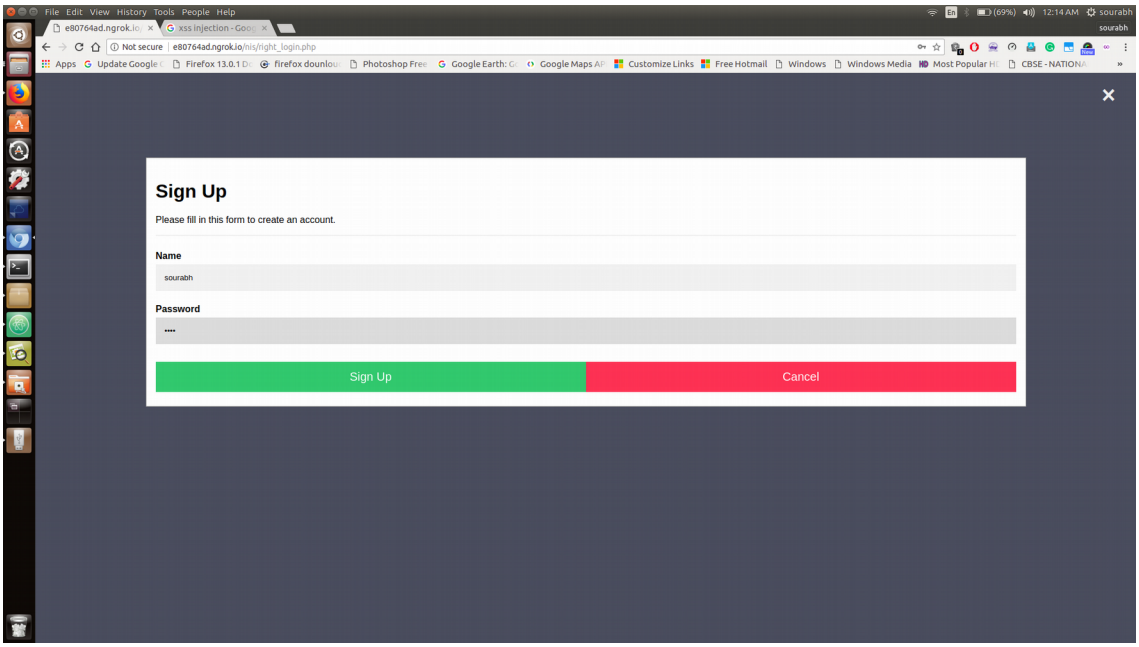
CRACKING PASSWORD



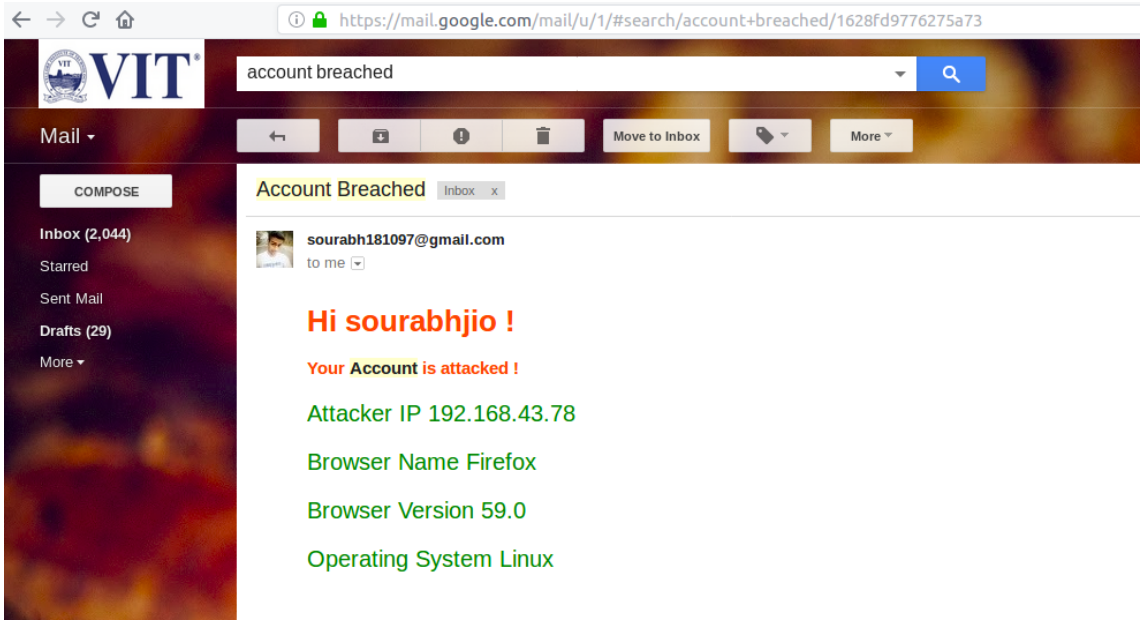
CALCULATE HASH



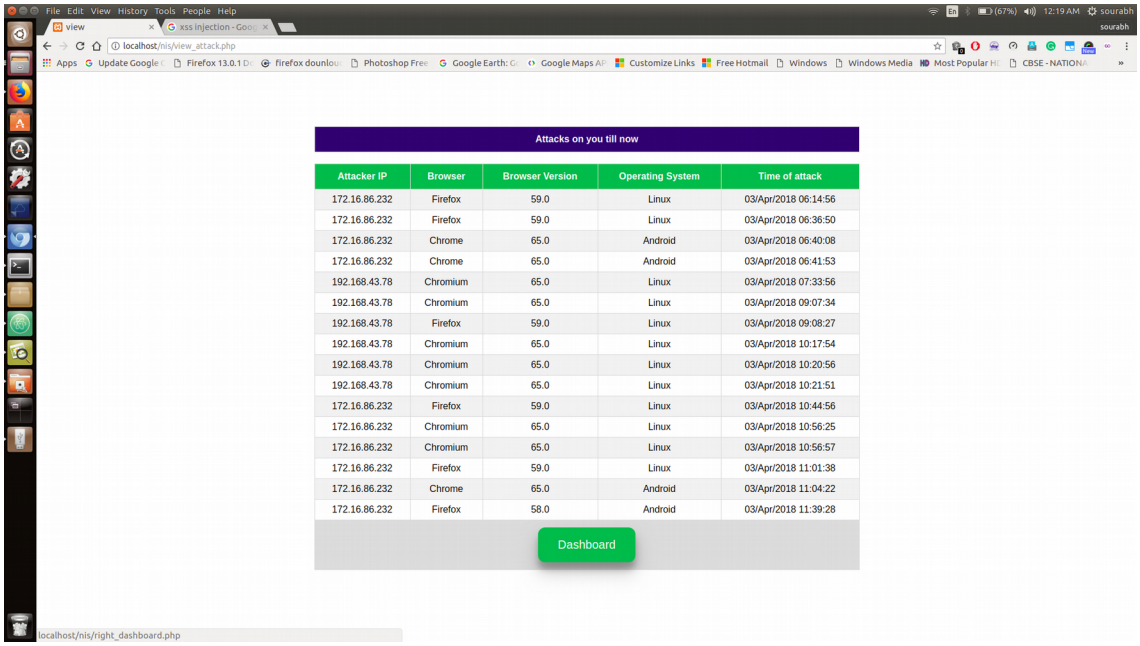
SIGN UP



SECURITY WARNING VIA EMAIL:



VIEW ATTACKs:



Attacks on you till now

Attacker IP	Browser	Browser Version	Operating System	Time of attack
172.16.86.232	Firefox	59.0	Linux	03/Apr/2018 06:14:56
172.16.86.232	Firefox	59.0	Linux	03/Apr/2018 06:36:50
172.16.86.232	Chrome	65.0	Android	03/Apr/2018 06:40:08
172.16.86.232	Chrome	65.0	Android	03/Apr/2018 06:41:53
192.168.43.78	Chromium	65.0	Linux	03/Apr/2018 07:33:56
192.168.43.78	Chromium	65.0	Linux	03/Apr/2018 09:07:34
192.168.43.78	Firefox	59.0	Linux	03/Apr/2018 09:08:27
192.168.43.78	Chromium	65.0	Linux	03/Apr/2018 10:17:54
192.168.43.78	Chromium	65.0	Linux	03/Apr/2018 10:20:56
192.168.43.78	Chromium	65.0	Linux	03/Apr/2018 10:21:51
172.16.86.232	Firefox	59.0	Linux	03/Apr/2018 10:44:56
172.16.86.232	Chromium	65.0	Linux	03/Apr/2018 10:56:25
172.16.86.232	Chromium	65.0	Linux	03/Apr/2018 10:56:57
172.16.86.232	Firefox	59.0	Linux	03/Apr/2018 11:01:38
172.16.86.232	Chrome	65.0	Android	03/Apr/2018 11:04:22
172.16.86.232	Firefox	58.0	Android	03/Apr/2018 11:39:28

Dashboard

CONCLUSION:

Our intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. While anomaly detection and reporting is the primary function, our intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses. Our IDS detect the activity and then send mail to concern individual about the intrusion done by any intruder or hacker.

THANK YOU