Cryptography Session No.2

Summary 20-07-2022

- Crypto + Graphy = Hidden/Secret + Writing
- Cryptography Knowledge helps in the security of all the technologies like Cloud, DevOps, Linux
- When a packet is traveling between the Client and server then these packets are called “Packets in transit”

- First go to the AWS cloud and create one instance after that take the public IP address and log into the git bash

```
Vimal Daga@DESKTOP-3E1AGGT MINGW64 ~
$ cd Downloads/

Vimal Daga@DESKTOP-3E1AGGT MINGW64 ~/Downloads
$ ssh  -i  aws_training_2022_key.pem   ec2-user@35.154.228.220
The authenticity of host '35.154.228.220 (35.154.228.220)' can't be established.
ED25519 key fingerprint is SHA256:oXtvUMmDj3Bj4+NerfiD5HPGQ+MX77DYGUWmAFj6Y4Q.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '35.154.228.220' (ED25519) to the list of known hosts
.
[ec2-user@ip-172-31-13-252 ~]$ sudo su - root
[root@ip-172-31-13-252 ~]# whoami
root
[root@ip-172-31-13-252 ~]# yum install  httpd
```

- Then give root power with the Sudo su – command
- To install Httpd in Redhat Linux- #yum install httpd
- To start httpd server- #systemctl start httpd

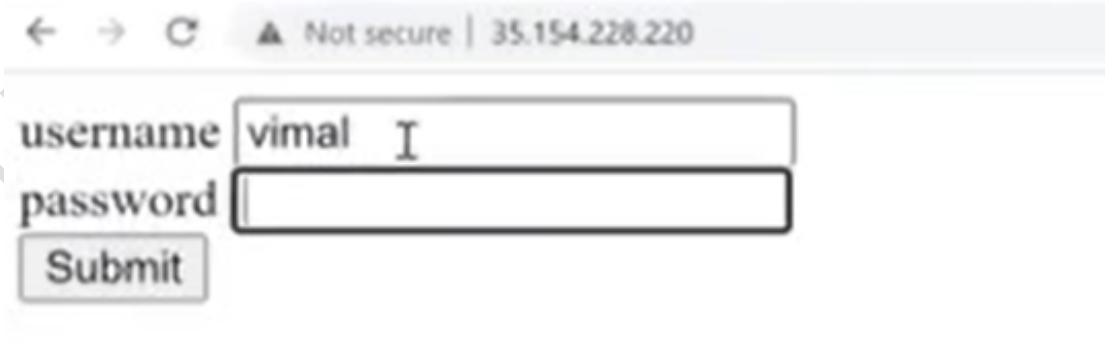
```
[root@ip-172-31-13-252 ~]# systemctl start httpd
[root@ip-172-31-13-252 ~]# cd /var/www/html/
[root@ip-172-31-13-252 html]# ls
[root@ip-172-31-13-252 html]# cat > index.html
this is LW
[root@ip-172-31-13-252 html]# cat index.html
this is LW
[root@ip-172-31-13-252 html]#
```

- After that create a simple login page
- Go the file

```
[root@ip-172-31-13-252 html]# vi index.html
```

```
<form method="POST">
username <input name="u" />
<br />
password <input name="p" type="password" />
<br />
<input type="submit" />
</form>
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq
```

- After copying the public IP address and paste on the browser



- But this website is not secure to secure this website we use Wireshark
- Wireshark is a tool, That can capture any network interfaces
- Download Wireshark- https://www.wireshark.org/download.html
- HTTPS is a secure protocol and Data is encrypted here.

- HTTP is a nonsecure protocol and data gets transferred in plain text format between client and server, So Anyone in between can sniff this packet and read the sensitive data.
- #nslookup "google.com" - It will print the IP address associated with this domain
- Encryption- The process of converting information or data into a code using some algorithms, Mainly to prevent unauthorized access and secure sensitive data.
- For Encryption, We have multiple algorithms available, One of the famous and powerful algorithms is AES.
- Openssl is a tool With which we can use these encryption algorithms(such as AES, and DES) to encrypt our data. By default, It will be pre-installed in your Redhat Linux
- vim plain.txt-> REDHAT #creating a plain.txt file with some sensitive data
- **#openssl enc -in plain.txt -aes256 -e -out secure.txt** -> Now this command will encrypt the data stored in the plain.txt file using the "aes256" encryption algorithm and will save the encrypted data in a new file "secure.txt"

```
[root@ip-172-31-13-252 ~]# openssl  enc  -in plain.txt  -aes256  -e  -out secure.txt
```

- While running the above command, it will ask you to create a password(key) which we will be using at the time of decrypting this data.

- **#openssl enc -in secure.txt -aes256 -d -out unsecure.txt** -> Now this command will load the "secure.txt" file and will decrypt the data inside it using the same algorithm i.e aes256, and will save the decrypted plain text data in "unsecure.txt"

```
openssl  enc -in  secure.txt  -aes256  -d  -out  p.txt
```

- We have two types of encryption
  - Symmetric Key Encryption -> Here we use the same key for locking and unlocking
  - Asymmetric Key Encryption- Here we have two different keys, i.e private and public key
- Here in our further discussion, we are discussing Symmetric Key Encryption only, In future classes, Asymmetric Encryption will be explained.

- **Monoalphabetic Substitution**-> Monoalphabetic Substitution is a substitution in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'I', for any number of occurrences in that plaintext, 'A' will always get encrypted to 'I'
- **Polyalphabetic Substitution**- A polyalphabetic cipher is any cipher based on substitution, using several substitution alphabets. In polyalphabetic substitution ciphers, the plaintext letters are enciphered differently based on their installation in the text. Rather than one-to-one correspondence, there is a one-to-many relationship between each letter and its substitutes.
- The polyalphabetic substitution technique was used in the Second World War by the Germans to encrypt their data.
- NIST is the community that has made some Data encryption Standards.