EXPERIMENT- 1

AIM: Write a program for Caesar Cipher for both Encryption andDecryption.

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus, to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1, Z = 25.

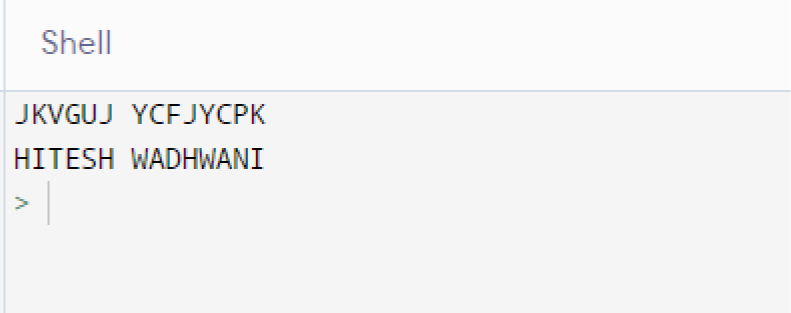
Encryption of a letter by a shift n can be described mathematically as.

INPUT -

```
def encrypt(key, message):
    message = message.upper()
    alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    result = ""

    for letter in message:
        if letter in alpha: #if the letter is actually a letter
            #find the corresponding ciphertext letter in the alphabet
            letter_index = (alpha.find(letter) + key) % len(alpha)

            result = result + alpha[letter_index]
        else:
            result = result + letter

    return result
```

```
def decrypt(key, message):
    message = message.upper()
    alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    result = ""

    for letter in message:
        if letter in alpha: #if the letter is actually a letter
            #find the corresponding ciphertext letter in the alphabet
            letter_index = (alpha.find(letter) - key) % len(alpha)

            result = result + alpha[letter_index]
        else:
            result = result + letter

    return result

print(encrypt(2, "hitesh Wadhwani"))
print(decrypt(2, “JKVGUJ YCFJYCPK”))
```

OUTPUT –



```
JKVGUJ YCFJYCPK
HITESH WADHWANI
>
```

Questions :

1) can we hide the actual message without changing its content?
2) major drawback of ceasar cipher?
3) is ceasar cipher symmatric or assymetric encryption ?, why ?
4) Encrypt the word alphabet using a caeser cipher with a shift of 3.

EXPERIMENT- 2

AIM: Write a program for RSA (Rivest-Shamir-Adleman encryption) algorithm.

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e., Public Key and Private Key. As the name describes, the Public Key is given to everyone, and the Private key is kept private.

An example of asymmetric cryptography:

- A client (for example browser) sends its public key to the server and requests some data.
- The server encrypts the data using the client's public key and sends the encrypted data.
- The client receives this data and decrypts it.

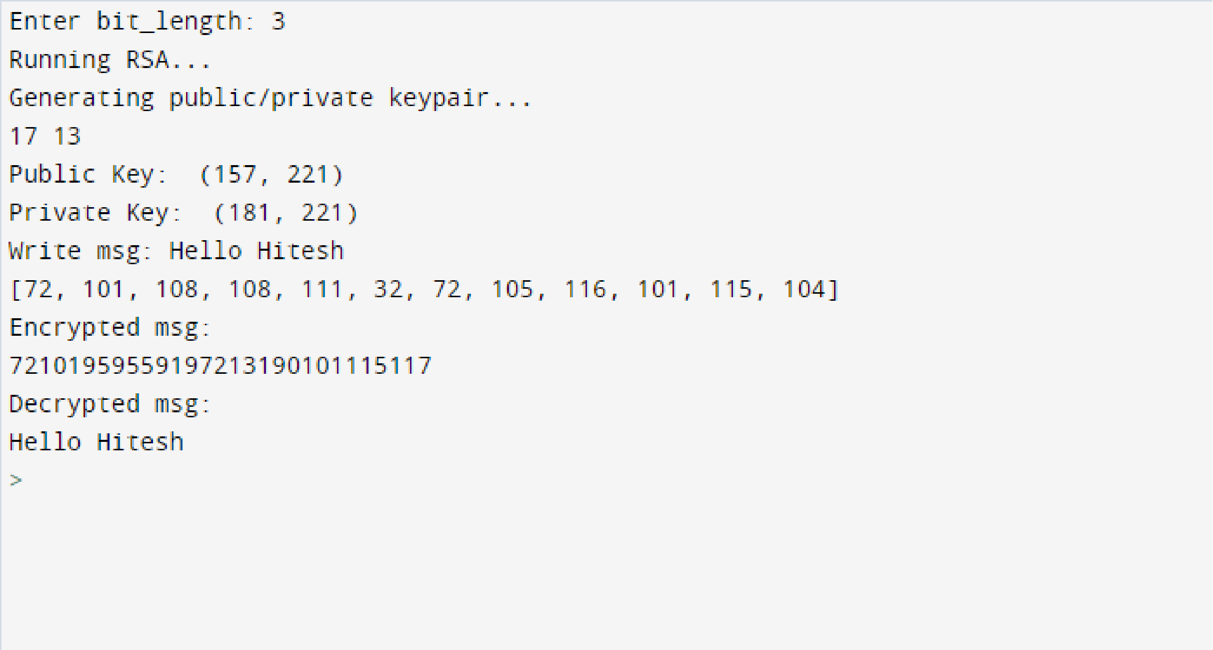
Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the public key of the browser.

The idea! The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is a multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So, if somebody can factorize the large number, the private key is compromised. Therefore, encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Input -

```
from math import sqrt
import random
from random import randint as rand

def gcd(a, b):
    if b == 0:
        return a
    else:
        return gcd(b, a % b)

def mod_inverse(a, m):
    for x in range(1, m):
        if (a * x) % m == 1:
            return x
    return -1

def isprime(n):
    if n < 2:
        return False
    elif n == 2:
        return True
    else:
        for i in range(2, int(sqrt(n)) + 1, 2):
            if n % i == 0:
                return False
    return True

p = rand(1, 1000)
q = rand(1, 1000)


def generate_keypair(p, q, keysize):

    nMin = 1 << (keysize - 1)
    nMax = (1 << keysize) - 1
    primes = [2]
    start = 1 << (keysize // 2 - 1)
    stop = 1 << (keysize // 2 + 1)

    if start >= stop:
        return []

    for i in range(3, stop + 1, 2):
        for p in primes:
            if i % p == 0:
                break
        else:
            primes.append(i)

    while (primes and primes[0] < start):
        del primes[0]

    while primes:
        p = random.choice(primes)
        primes.remove(p)
        q_values = [q for q in primes if nMin <= p * q <= nMax]
        if q_values:
            q = random.choice(q_values)
            break
    print(p, q)
    n = p * q
    phi = (p - 1) * (q - 1)

    e = random.randrange(1, phi)
    g = gcd(e, phi)

    while True:
        e = random.randrange(1, phi)
        g = gcd(e, phi)
        d = mod_inverse(e, phi)
        if g == 1 and e != d:
            break
    return ((e, n), (d, n))

def encrypt(msg_plaintext, package):
    e, n = package
    msg_ciphertext = [pow(ord(c), e, n) for c in msg_plaintext]
    return msg_ciphertext

def decrypt(msg_ciphertext, package):
    d, n = package
    msg_plaintext = [chr(pow(c, d, n)) for c in msg_ciphertext]
    return (".join(msg_plaintext))

bit_length = int(input("Enter bit_length: "))
print("Running RSA...")
print("Generating public/private keypair...")
public, private = generate_keypair(p, q, 2**bit_length)  # 8 is the keysize (bit-length) value.
print("Public Key: ", public)
print("Private Key: ", private)
msg = input("Write msg: ")
print([ord(c) for c in msg])
encrypted_msg = encrypt(msg, public)
print("Encrypted msg: ")
print(".join(map(lambda x: str(x), encrypted_msg)))
print("Decrypted msg: ")
print(decrypt(encrypted_msg, private)
```

output -



```
Enter bit_length: 3
Running RSA...
Generating public/private keypair...
17 13
Public Key:  (157, 221)
Private Key:  (181, 221)
Write msg: Hello Hitesh
[72, 101, 108, 108, 111, 32, 72, 105, 116, 101, 115, 104]
Encrypted msg:
72101959559197213190101115117
Decrypted msg:
Hello Hitesh
>
```

Question –

1.What is full form of RSA
2.Why is cracking of RSA impossible
3.What is hashing
4.What is a one way function

EXPERIMENT- 3

AIM: Case study of any Indian I.T. Act.

Objectives of the Act

The Information Technology Act, 2000 provides legal recognition to the transaction made via electronic exchange of data and other electronic means ofcommunication or electronic commerce transactions.

This also involves the use of alternatives to a paper-based method of communication and information storage to facilitate the electronic filing ofdocuments with the Government agencies.

Further, this act amended the Indian Penal Code 1860, the Indian Evidence Act1872, the Bankers' Books Evidence Act 1891, and the Reserve Bank of India Act 1934. The objectives of the Act are as follows:

i. Grant legal recognition to all transactions done via electronic exchange ofdata or other electronic means of communication or e-commerce, in placeof the earlier paper-based method of communication.

ii. Give legal recognition to digital signatures for the authentication of anyinformation or matters requiring legal authentication

iii. Facilitate the electronic filing of documents with Government agenciesand also departments

iv. Facilitate the electronic storage of data

v. Give legal sanction and also facilitate the electronic transfer of fundsbetween banks and financial institutions

vi. Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accountsin electronic form.

Features of the Information Technology Act, 2000

a. All electronic contracts made through secure electronic channels arelegally valid.

b. Legal recognition for digital signatures.

c. Security measures for electronic records and also digital signatures are inplace

d. A procedure for the appointment of adjudicating officers for holdinginquiries under the Act is finalized

e. Provision for establishing a Cyber Regulatory Appellant Tribunal underthe Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.

f. An appeal against the order of the Cyber Appellant Tribunal is possibleonly in the High Court

g. Digital Signatures will use an asymmetric cryptosystem and also a hashfunction

h. Provision for the appointment of the Controller of Certifying Authorities(CCA) to license and regulate the working of Certifying Authorities. TheController acts as a repository of all digital signatures.

i. The Act applies to offences or contraventions committed outside India

j. Senior police officers and other officers can enter any public place andsearch and arrest without warrant

k. Provisions for the constitution of a Cyber Regulations AdvisoryCommittee to advise the Central Government and Controller.

Applicability and Non-Applicability of the Act

Applicability:

According to Section 1 (2), the Act extends to the entire country, which also includes Jammu and Kashmir. In order to include Jammu and Kashmir, the Actuses Article 253 of the constitution. Further, it does not take citizenship into account and provides extra-territorial jurisdiction.

Section 1 (2) along with Section 75, specifies that the Act is applicable to any offence or contravention committed outside India as well. If the conduct of person constituting the offence involves a computer or a computerized system or network located in India, then irrespective of his/her nationality, the person ispunishable under the Act.

Lack of international cooperation is the only limitation of this provision.

Non-Applicability:

According to Section 1 (4) of the Information Technology Act, 2000, the Act isnot applicable to the following documents:

1. Execution of Negotiable Instrument under Negotiable Instruments Act,1881, except cheques.

2. Execution of a Power of Attorney under the Powers of Attorney Act,1882.
3. Creation of Trust under the Indian Trust Act, 1882.
4. Execution of a Will under the Indian Succession Act, 1925 including any other testamentary disposition
   by whatever name called.
5. Entering into a contract for the sale of conveyance of immovable propertyor any interest in such property.
6. Any such class of documents or transactions as may be notified by the Central Government in the Gazette.

- What is the Indian IT act?

  It's an act passed by the government of India to deal with cybercrimes andcyber bullying or electronic bullying.

- When was this act passed?

  The bill was passed in the budget session of 2000.

- Why was this act passed?

  It was passed to deal with the increasing cybercrimes and electronicbullying.

CASE STUDY- 1

State Of Tamil Nadu v/s Suhas Katti Conviction Within 7 Months

An incident involving the posting of obscene, defamatory, and irritating messages about a divorced woman in the Yahoo Messages group. E-mails werealso sent providing information to the victim through a false e-mail address opened by the accused in the victim's name. After the message was made public, she called a woman she thought was being bullied and she was bullied.

Defendant said her victim was a known friend of her family and wanted to marry her. But she married another man. This marriage later ended in divorceand the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

The accused is found guilty and convicted of offenses under sections 469, 509 IPC, and 67 of the IT Act 2000. This is considered the first case convicted undersection 67 of the Information Technology Act 2000 in India.

"The accused is found guilty of offenses under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offense to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offense u/s 509 IPC sentenced to undergo 1-year Simple imprisonment and to pay fine of Rs.500/- and for the offense u/s 67 of IT Act 2000 to undergo RI for2 years and to pay fine of Rs.4000/ All sentences to run concurrently."

The accused paid the fine amount and was lodged at Central Prison, Chennai. This is considered the first conviction under section 67 of the Information Technology Act 2000 in India.

Section 469 in The Indian Penal Code

469. Forgery for purpose of harming reputation. —Whoever commits forgery, 1[intending that the document or electronic record forged] shall harm the repu-tation of any party, or knowing that it is likely to be used for that purpose, shallbe punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

509B. Sexual harassment by electronic mode.

Whoever, by means of telecommunication device or by any other electronic mode including internet, makes creates, solicits or initiates the transmission of any comment, request, suggestion, proposal, image or other communication, which is obscene, lewd, lascivious, filthy or indecent with intent to harass or cause or having knowledge that it would harass or cause annoyance or mentalagony to a woman shall be punished with rigorous imprisonment for a term which shall not be less than six months but may extend to two years and shall also be liable to fine."

CASE STUDY- 2

Amar Singh v Union of India [(2011) 4 AWC 3726 SC]

In this case, the applicant claimed that his or her phone was intercepted by the mobile operator. He argued that the wiretapping charge violated the basic rightto privacy under Article 21 of the Indian Constitution.

The service provider claimed that it was carrying out government orders. This case is significant with respect to sections 69, 69A, and 69B of the InformationTechnology Act of 2000. The court noted that telecommunications carriers perform functions of a public nature. It is his inalienable duty to act prudently and responsibly.

Additionally, if government orders called "intercept calls" contain mistakes, service providers are required to verify the authenticity of these orders. Thecourt also directed the central government to develop specific guidelines/guidelines to prevent unauthorized phone interception.

Section 69. Power to issue directions for interception or monitoring ordecryption of any information through any computer resource.

Section 69A. Power to issue directions for blocking public access of any information through any computer resource.

Section 69B. Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

EXPERIMENT- 4

AIM: Compare security features of at least three web browsers**.**

Safari has been designed from the ground up to protect user privacy. Key privacy features like Intelligent Tracking Prevention (ITP) and fingerprinting defense are turned on by default, so there is no need to make changes in Settings or Safari preferences to benefit from these privacy protections. Safari minimizes the amount of data collected by Apple and shared with third parties. Where possible, Safari's privacy protections are designed to process data on device. For example, ITP uses machine learning to classify tracking data locally so that browsing history isn't sent to Apple. Safari also limits the amount of information passed to search engines when a user search using the Smart Search field. And Safari is designed to provide users with transparency and control around data that is shared. For example, if a user visits a website that wants to access location using Location Services on the device, or use the camera or microphone, Safari will ask permission from the user before granting access. Users can also customize these settings for each website to allow, not allow, or ask each time the site is visited. Safari is designed to hide the user's identity when sharing information with Apple. Analytics data shared with Apple is not attached to identifying information and, in some cases, is protected using differential privacy, a technique that obscures individual information while allowing Apple to analyze broader trends in web-browsing behavior. And Safari implements security best practices to protect user data.

Security Features of Safari:

a) **Privacy by Design-** Safari has been designed from the ground up to protect user privacy. Key privacy features like Intelligent Tracking Prevention (ITP) and fingerprinting defense are turned on by default, so there is no need to make changes in Settings or Safari preferences to benefit from these privacy protections.

b) **Protection from cross-site tracking-** In the years since the web was created, technology has been developed to track user behavior across websites for advertising purposes. Users experience this tracking in action when they look at a product online and then ads for that product seem to follow them around the web. Tracking is pervasive; some websites include 100 or more trackers from different companies on a single page.

c) **Ad measurement that respects user privacy-** Apple understands that advertising is important for the economy of the web. Online advertising should not require privacy-invasive tracking and neither should advertising measurement. Unfortunately, ad click measurement has traditionally used tracking technology that infringes on user privacy.

d) **Minimizing data sharing with the Smart Search field-** The Safari Smart Search field enables a user to type website names, URLs, and search queries into one easy-to-use field at the top of the browser window. As the user types, it includes Safari suggestions for recommended websites, shows results from the user's bookmarks, history, and tabs, and provides relevant information from sources like Wikipedia.

e) **Browsing privately-** Users sometimes want to keep their browsing data private from the people they share the device with or from people on a public device. Safari was the first browser to introduce a Private Browsing mode, which was first shipped in 2005. When a user search using a Private Browsing window, Safari doesn't save a list of the web pages visited, add typed information to AutoFill, or store the list of downloads and searches in the Smart Search field (though downloaded items remain on the device). This means that users on a shared device won't be able to see which sites other users visited, what they searched for, or what they typed into web forms.

f) **Deleting history and other data-** Outside of Private Browsing sessions, Safari saves history and website data to the device to enable helpful functionality, like allowing users to access their browsing history. This saved information includes a history of which pages have been visited, search history, as well as cookies and other website data like signin information. To provide the user control over what is saved on a device, Safari makes it easy to delete this data. With the Clear History feature, users can clear history and website data (including cookies) for the time period they choose.

g) **Secure payments on the web-** Shopping online is one of the most common things that users do in a web browser. To make the process of paying easy, Safari provides seamless integration with Apple Pay, a payment method that is designed to protect privacy. In addition to web-based tracking, payments are also a major source of information for the data industry. For example, when a user makes a purchase with a physical credit card, information about the payment may be passed to companies that build profiles on users based on what they buy.

- **Google Chrome**

Google Chrome is one of the best browsers (not for security) And is most used by over 1 billion people around the world. Google chrome has tons of features like Extenstions and Google currents(formerly known as google+).
Im not saying that you should use Google Chrome as your main browser because browsers like FireFox and Edge are good alternatives for security.

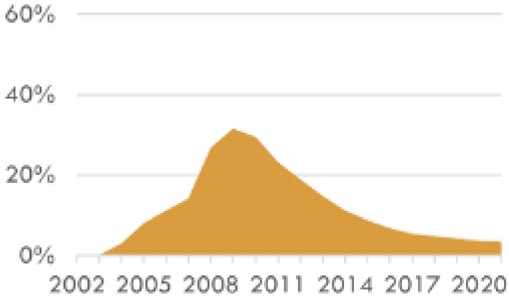
Security Features of Google Chrome:

a) **Auto Update-**
The most important step is to keep your browser up-to-date with the latest security patches. An older version of the browser can have many severe vulnerabilities that can be exploited remotely. By default, Chrome has the auto-update feature. It can automatically update to the latest version and ask for browser restart when it is done. In case it is not updating automatically.

b) **Proactive security alerts help protect your private information-**
We'll proactively notify you if we detect something that we think you should know about – like a suspicious login or a malicious website, file or app – and we'll provide guidance to help you stay better protected. When we detect something suspicious in your account, we'll send a notification to your inbox or phone so that you can protect your account with one click.

c) **Threats detected and blocked automatically-**
Safe Browsing protects four billion devices every day, including yours. To make the Internet safer for everyone, we made this technology available free of cost for other companies to use in their browsers, including Apple's Safari and Mozilla's Firefox. So you're protected as you browse on Google and beyond.

➢ **Mozilla Firefox**



Strongest in Europe; negligible on mobile devices

Mozilla Firefox, or simply Firefox, is a free and open-source[19] web browser developed by the Mozilla Foundation and its subsidiary, the Mozilla Corporation. It uses the Gecko rendering engine to display web pages, which implements current and anticipated web standards.[20] In November 2017, Firefox began incorporating new technology under the code name Quantum to promote parallelism and a more intuitive user interface.[21] Firefox is available for Windows 7 and later versions, macOS, and Linux. Its unofficial ports are available for various Unix and Unix-like operating systems, including FreeBSD,[8] OpenBSD,[9] NetBSD,[10] illumos,[11] and Solaris Unix.[13] It is also available for Android and iOS. However, as with all other iOS web browsers, the iOS version uses the WebKit layout engine instead of Gecko due to platform requirements. An optimized version is also available on the Amazon Fire TV, as one of the two main browsers available with Amazon's Silk Browser.[22]

Firefox was created in 2002 under the code name "Phoenix" by the Mozilla community members who desired a standalone browser, rather than the Mozilla Application Suite bundle. During its beta phase, it proved to be popular with its testers and was praised for its speed, security, and add-ons compared to Microsoft's then-dominant Internet Explorer 6. It was released on November 9, 2004,[23] and challenged Internet Explorer's dominance with 60 million downloads within nine months.[24] It is the spiritual successor of Netscape Navigator, as the Mozilla community was created by Netscape in 1998 before their acquisition by AOL.[25]

Firefox usage share grew to a peak of 32.21% in November 2009,[26] with Firefox 3.5 overtaking Internet Explorer 7, although not all versions of Internet Explorer as a whole;[27][28] its usage then declined in competition with Google Chrome.[26] As of September 2022, according to StatCounter, it has 7.4% usage share as a desktop web browser, making it the fourth-most popular desktop web browser after Google Chrome (67%), Microsoft Edge (11%), and Safari (8.8%).[29] Across all platforms it again places fourth though with a usage share of 3.2%

Security Features of Mozilla Firefox:

a) **Password Management-**
A password manager should help you create strong passwords and protect them across accounts.

b) **Tracking Protection-**
Following doesn't make anyone feel safe, even if it's an annoying ad following you on the web. Blocking third-party trackers can help by not allowing the annoying "cookies" track that enables ads.

c) **Private Browsing-**

Speaking of private browsing, it’s a powerful privacy tool that’s easy to use. On Firefox, private browsing means we don’t save information about where you’ve been, clicked, or looked.

d) **Do Not Track-**

If you want to make sure that sites are not collecting information about what you buy or browse, you can opt-out of behavioral tracking, and those sites will not be able to track and sell your behavior.

e) **Instant Website ID-**

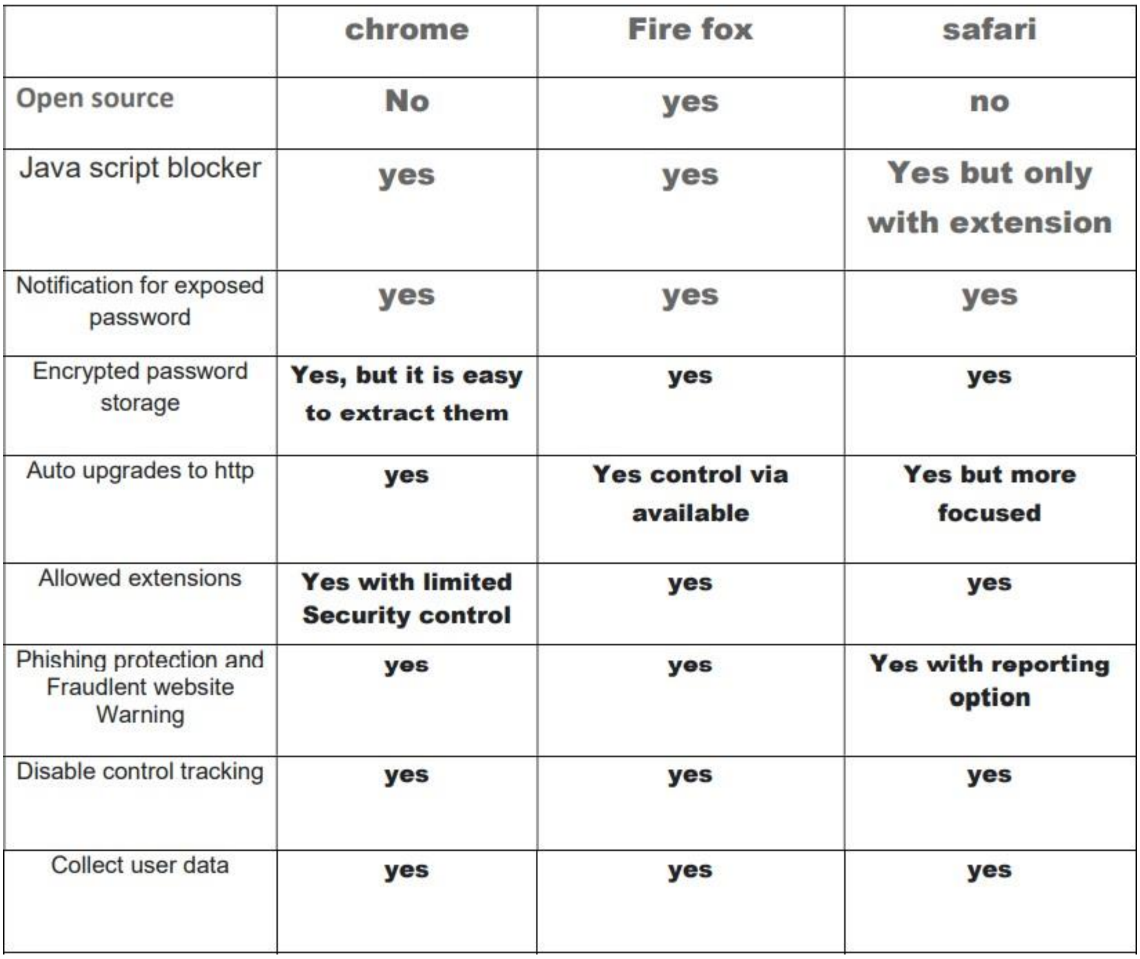
Click on a site’s favicon, and you can see information about the site’s identity. With one click you can find out whether or not a site is legitimate and check a site out before you make a purchase or share sensitive information.

f) **Containers-**

Cleaning up your online space isn’t just good feng shui, it can lessen the worry of being tracked. Separate identities for your work websites or your personal interests keep trackers confined to one area. Ads that have nothing to do with work won’t pop-up in the middle of a presentation. For this purpose, we created Containers. Containers help you stay organized and keep trackers in their place. Checking flight prices? Log onto the samewebsite on different containers to make sure the price doesn’t mysteriously go up the second time you visit.

g) **Firefox Monitor-**

It’s hard to go a week without hearing of a new data breach. If you’re a human who lives and works, you probably don’t have the time to keep track of data news. We thought it might be nice to have a tool that kept watch on accounts and could let you know if anything fishy is going on.Firefox Monitor does just that, and you don’t need to use the Firefox browser to sign up. Simply enter your email to see if it’s been compromised and get alerts for new hacks



	chrome	Fire fox	safari
Open source	No	yes	no
Java script blocker	yes	yes	Yes but only with extension
Notification for exposed password	yes	yes	yes
Encrypted password storage	Yes, but it is easy to extract them	yes	yes
Auto upgrades to http	yes	Yes control via available	Yes but more focused
Allowed extensions	Yes with limited Security control	yes	yes
Phishing protection and Fraudlent website Warning	yes	yes	Yes with reporting option
Disable control tracking	yes	yes	yes
Collect user data	yes	yes	yes

Questions:

1. What are cookies
2. Why are cookies dangerous to keep saved.
3. How autocomplete features in browsers are a threat to security.
4. What are the four most prevalent security threats in browsers.

EXPERIMENT- 5

AIM: Finding out Vulnerable data on E-commerce Websites.

- **Akamai**
  - Last month two Italian security researchers revealed they had netted more than $46,000 in bug bounties after discovering a misconfiguration vulnerability in **Akamai** – despite receiving nothing from Akamai itself.
  - The exploit, which leveraged HTTP smuggling and hop-by-hop header abuse techniques, instead achieved payouts from several of the company's customers. These included $25,200 from PayPal and rewards from Airbnb, Hyatt Hotels, Valve, Zomato, and Goldman Sachs.
  - In other payout news, researcher Saajan Bhujel bagged a $10,000 bounty from **GitHub** after finding a way to spoof the platform's login interface. Bypassing HTML filtering in the MathJax display engine allowed him to inject form elements and change the website's CSS, potentially fooling users into entering credentials into a fake login page.

- **Eastern Front**

  - Geo-political factors as well as the security policy of e-commerce providers can impact the availability of products for illicit shops, which also impacts the overall landscape.
  - For example, more countries adopt security chips instead of magnetic stripes in their payment systems, meaning that magnetic strip card data dumps have less utility. Data dumps containing card info plus CVV values however have greater utility because they enable online fraud.
  - Chris Morgan, senior cyber threat intelligence analyst at Digital Shadows, told *The Daily Swig* that sanctions against Russia following its invasion of Ukraine in February have impeded the ability of cybercriminals to realize the profits from their illegal activity.

Phishing and Malware

Phishing scams remain popular with hackers despite companies' educational and awareness efforts. In this method, a hacker sends an email to an employee,often posing as a colleague and trying to persuade the employee to click on a malicious link or reveal sensitive information like passwords or credit card numbers.

Phishing is a common technique for installing malware on a device; once an employee has clicked the link, the malware can infect your system and beginaccessing your sensitive data.

Bad Bots

Bots can make your life easier by automating simple tasks, but they can makehackers' jobs easier too. Cybercriminals increasingly use bots to harvest data,engage in price scraping, or perform other malicious actions that could harm your security and your business.

Such attacks include distributed denial of service (DDOS) attacks, where bots are deployed to overwhelm your site's capacity with traffic, allowing hackers toaccess your site while your focus is elsewhere.

Bots are also frequently used in brute force attacks, where algorithms methodically guess every possible password until they find the one that finallysucceeds.

Cross-Site Scripting and SQL Injections

Both SQL injections and Cross-Site Scripting (XSS attacks) seek to exploit existing vulnerabilities in your site with an injection of malicious code. SQLinjection occurs when hackers use a site's entry forms (such as email or password fields) to inject malicious code into your online store.

This code is then used to access and manipulate sensitive databases withinformation like phone numbers and credit card information. Cross-Site Scripting works in a similar way but targets web applications rather thanwebsite forms.

Resolving E-Commerce Security Issues

In the face of these threats, it’s important to perform due diligence and protect your company (and your customers’ information) to the best of your ability. Thefollowing techniques can help you improve your website security and mitigate losses that may occur.

Security Hygiene

Basic security measures can go a long way toward protecting your company from cyberattacks. All accounts should be secured with strong, unique passwords that are changed frequently. Multi-factor authentication is another popular way of adding another layer of security to your accounts. You can alsoarrange to receive notifications every time your system is accessed from an unknown IP address, which can alert you to potential breaches.

Questions:

1. What are financial frauds
2. How can a e commerce website be affected by spaming
3. What is XSS
4. Why https is better than http.

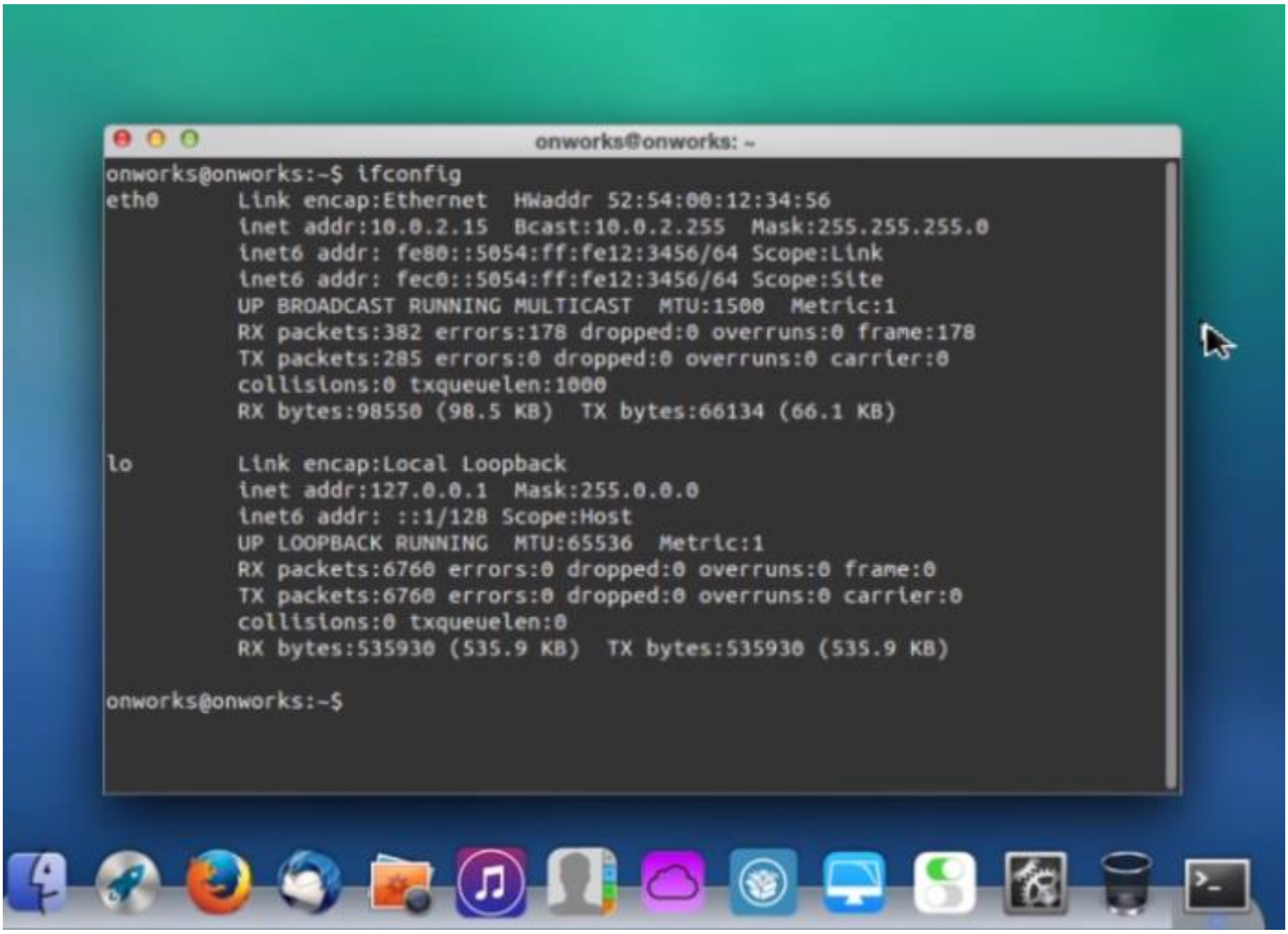
EXPERIMENT- 6

AIM: Computer Networking commands on Mac OS.

Command Name: ifconfig

Command: student$ curl ifconfig.me

- Just like on a Windows computer, you can use ipconfig on Mac with Terminal to find your local IP address. If you’re connected to the internet through a wireless network:
- Hit ⌘ + Space to search and open Terminal
- Type in ipconfig getifaddr en0
- Every device connected to your network including the router is assigned an internal IP address. Together, the entire network is assigned a single external IP address once it’s connected to the internet.

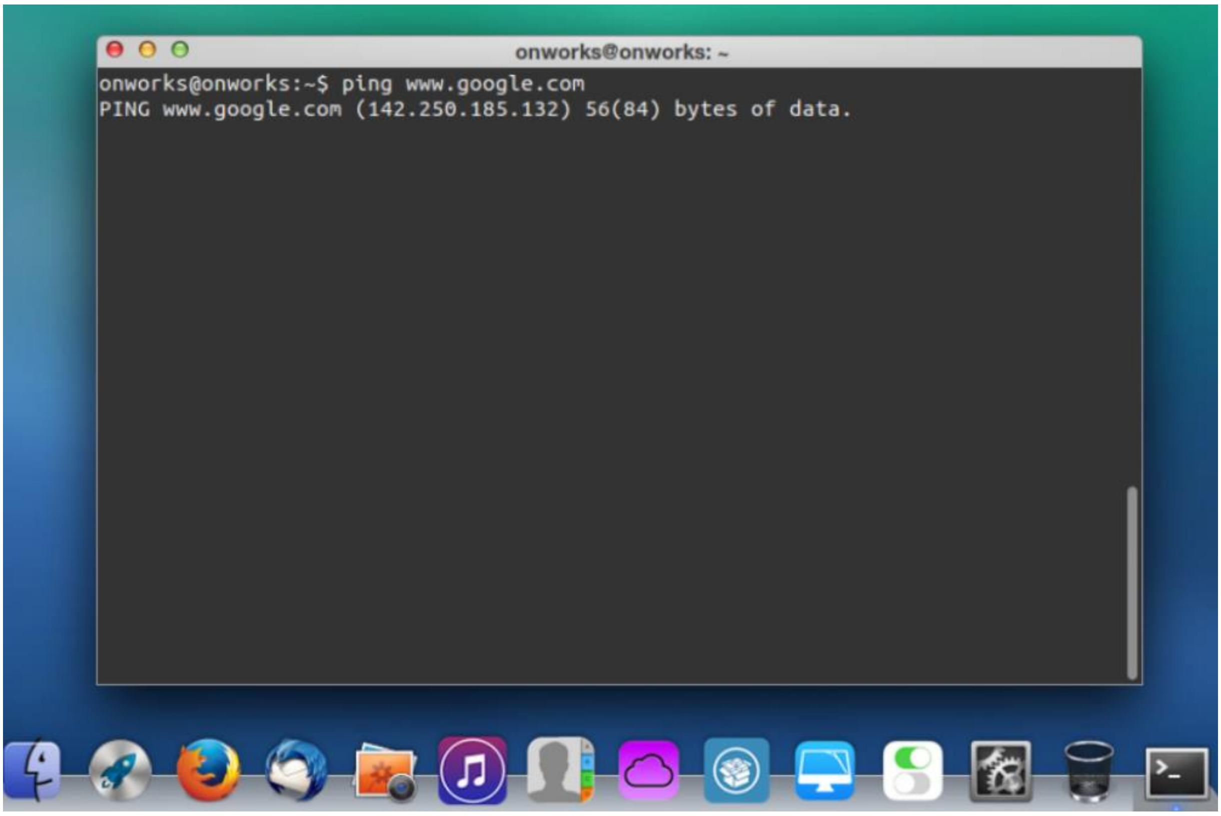


```
onworks@onworks:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:12:34:56
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe12:3456/64 Scope:Link
          inet6 addr: fec0::5054:ff:fe12:3456/64 Scope:Site
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:382 errors:178 dropped:0 overruns:0 frame:178
          TX packets:285 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:98550 (98.5 KB)  TX bytes:66134 (66.1 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:6760 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6760 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:535930 (535.9 KB)  TX bytes:535930 (535.9 KB)

onworks@onworks:~$
```

Command Name: Ping

Command: Ping 150.129.147.210

"Ping" tests if a computer is connected to a network. "Ping" also determines the latency or delay between two computers. It is used to ensure that a host computer which your computer tries to access is operating. A ping test is run for troubleshooting to know connectivity as wellas response time. Two MacOS applications to execute a "ping" test - Network Utility, Terminal command.



```
onworks@onworks:~$ ping www.google.com
PING www.google.com (142.250.185.132) 56(84) bytes of data.
```

Command Name: Netstat

Command: netstat -vanp tcp

- To run netstat and see detailed data about your Mac's network, open a new Terminal window, type netstat, and press Enter.
- Limit netstat's output with flags and options. To see netstat's available options, type man netstat at the command prompt.
- Filtering netstat's output is essential to understanding what's happening on your Mac's active ports. Netstat's built-in flags allow you to set options, limiting the command's scope.
- It's important to note that netstat on macOS doesn't work the same way as netstat on Windows and Linux. Using flags or syntax from those implementations of netstat may not result in the expected behavior.
- Useful Flags-

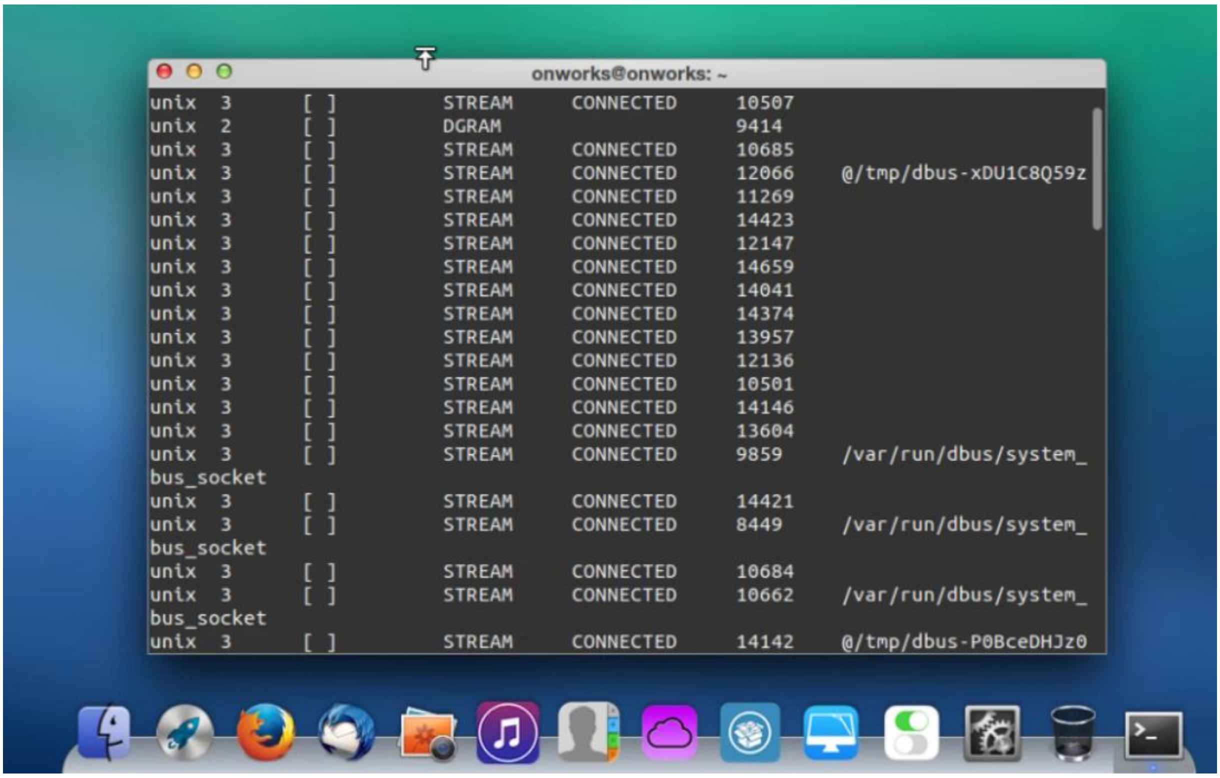
Here are some of the most commonly used flags:

(1) -a includes server ports in netstat's output, which are not included in the default output.

(2) -g displays information associated with multicast connections.

(3) -I interface provides packet data for the specified interface. All available interfaces can be viewed with the -i flag, but en0 is typically the default outgoingnetwork interface. (Note the lowercase letter.)

(4) -n suppresses the label of remote addresses with names. These speeds up netstat's output while eliminating only limited information.



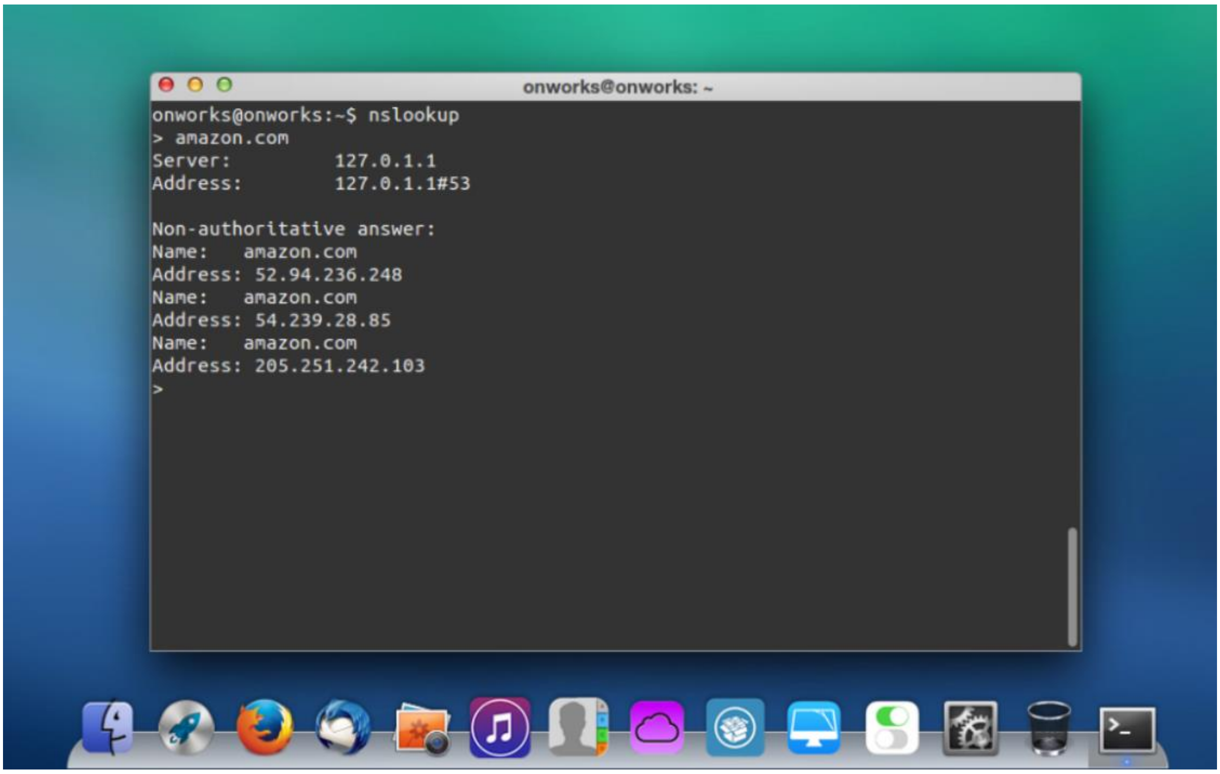
```
unix  3        [ ]         STREAM     CONNECTED     10507
unix  2        [ ]         DGRAM                    9414
unix  3        [ ]         STREAM     CONNECTED     10685
unix  3        [ ]         STREAM     CONNECTED     12066    @/tmp/dbus-xDU1C8Q59z
unix  3        [ ]         STREAM     CONNECTED     11269
unix  3        [ ]         STREAM     CONNECTED     14423
unix  3        [ ]         STREAM     CONNECTED     12147
unix  3        [ ]         STREAM     CONNECTED     14659
unix  3        [ ]         STREAM     CONNECTED     14041
unix  3        [ ]         STREAM     CONNECTED     14374
unix  3        [ ]         STREAM     CONNECTED     13957
unix  3        [ ]         STREAM     CONNECTED     12136
unix  3        [ ]         STREAM     CONNECTED     10501
unix  3        [ ]         STREAM     CONNECTED     14146
unix  3        [ ]         STREAM     CONNECTED     13604
unix  3        [ ]         STREAM     CONNECTED     9859     /var/run/dbus/system_
bus_socket
unix  3        [ ]         STREAM     CONNECTED     14421
unix  3        [ ]         STREAM     CONNECTED     8449     /var/run/dbus/system_
bus_socket
unix  3        [ ]         STREAM     CONNECTED     10684
unix  3        [ ]         STREAM     CONNECTED     10662    /var/run/dbus/system_
bus_socket
unix  3        [ ]         STREAM     CONNECTED     14142    @/tmp/dbus-P0BceDHJz0
```

Command Name: nslookup

Command: nslookup amazon.com, nslookup Ethereum.org

The nslookup command queries internet domain name servers in two modes. Interactive mode allows you to query name servers for information about various hosts and domains, orto print a list of the hosts in a domain. In noninteractive mode, the names and requested information are printed for a specified host or domain.

The nslookup command enters interactive mode when no arguments are given, or when the first argument is a - (minus sign) and the second argument is the host name or internet address of a name server. When no arguments are given, the command queries the default name server. The nslookup command enters non-interactive mode when you give the name orinternet address of the host to be looked up as the first argument. The optional second argument specifies the host name or address of a name server.



```
onworks@onworks:~$ nslookup
> amazon.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   amazon.com
Address: 52.94.236.248
Name:   amazon.com
Address: 54.239.28.85
Name:   amazon.com
Address: 205.251.242.103
>
```

Questions:

1. What is a network
2. What is a gateway or router
3. What is protocol
4. What is routing

EXPERIMENT- 7

AIM: STUDY OF WIRESHARK

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

How to Install Wireshark on Linux

If you have a Linux system, you'd install Wireshark using the following sequence (notice that you'll need to have root permissions):

```
$ sudo apt-get install wireshark

$ sudo dpkg-reconfigure wireshark-common

$ sudo usermod -a -G wireshark $USER

$ newgrp wireshark
```

Once you have completed the above steps, you then log out and log back in, and then start Wireshark:

```
$ wireshark &
```

What Is Wireshark Used For?

Wireshark has many uses, including troubleshooting networks that have performance issues. Cybersecurity professionals often use Wireshark to trace connections, view the contents of suspect network transactions and identify bursts of network traffic. It's a major part of any IT pro's toolkit – and hopefully, the IT pro has the knowledge to use it.

When Should Wireshark Be Used?

Wireshark is a safe tool used by government agencies, educational institutions, corporations, small businesses, and non-profits alike to troubleshoot network issues. Additionally, Wireshark can be used as a learning tool.

Those new to information security can use Wireshark as a tool to understand network traffic analysis, how communication takes place when particular protocols are involved and

where it goes wrong when certain issues occur. Of course, Wireshark can't do everything.

First of all, it can't help a user who has little understanding of network protocols. No tool, no matter how cool, replaces knowledge very well. In other words, to properly use Wireshark, you need to learn exactly how a network operates. That means, you need to understand things such as the three-way TCP handshake and various protocols, including TCP, UDP, DHCP and ICMP.

Second, Wireshark can't grab traffic from all of the other systems on the network under normal circumstances. On modern networks that use devices called switches, Wireshark (or any other standard packet-capturing tool) can only sniff traffic between your local computer and the remote system it is talking to.

Third, while Wireshark can show malformed packets and apply color coding, it doesn't have actual alerts; Wireshark isn't an intrusion detection system (IDS).

Fourth, Wireshark can't help with decryption with regards to encrypted traffic.

And finally, it is quite easy to spoof IPv4 packets. Wireshark can’t really tell you if a particular IP address it finds in a captured packet is a real one or not. That requires a bit more know-how on the part of an IT pro, as well as additional software.

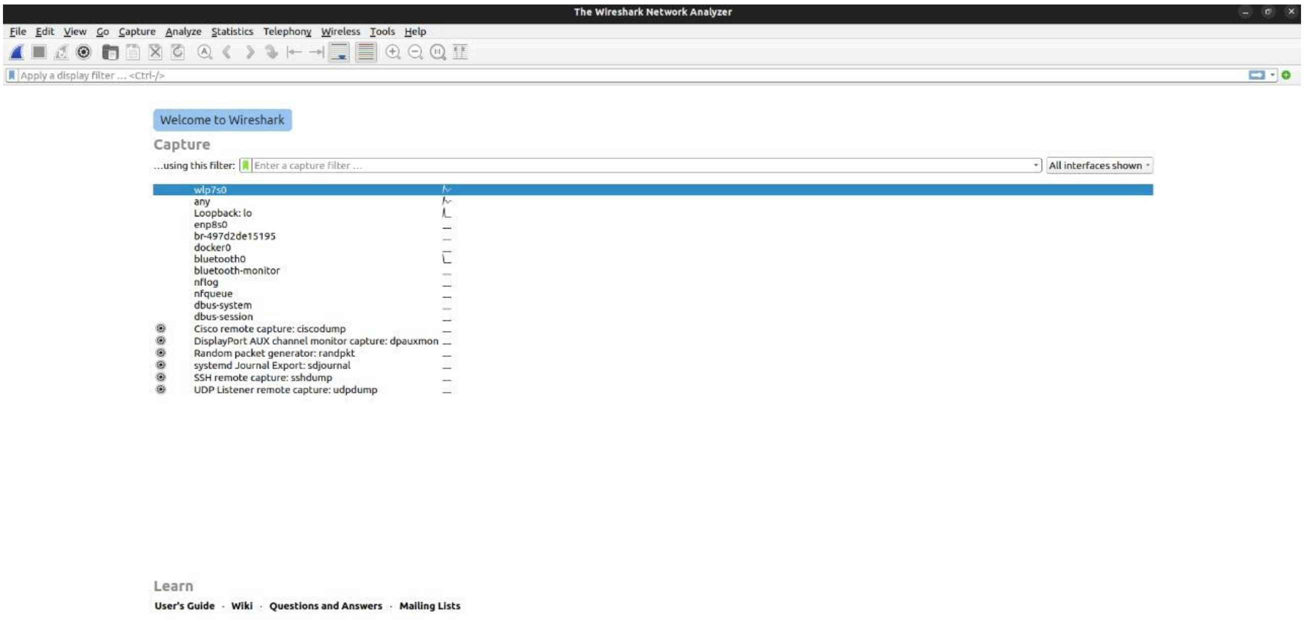
How to Capture Packets Using Wireshark

Once you’ve installed Wireshark, you can start grabbing network traffic. But remember: To capture any packets, you need to have proper permissions on your computer to put Wireshark into promiscuous mode.

- **In a Windows system, this usually means you have administrator access.**
- **In a Linux system, it usually means that you have root access.**

As long as you have the right permissions, you have several options to actually start the capture. Perhaps the best is to select Capture >> Options from the main window. This will bring up the Capture Interfaces window, as shown below in Figure 4. This window will list all available interfaces. In this case, Wireshark provides several to choose from. For this example, we’ll select the Ethernet 3 interface, which is the most active interface. Wireshark visualizes the traffic by showing a moving line, which represents the packets on the network. Once the network interface is selected, you simply click the Start button to begin your capture.

Capturing Real-time Data Packets -


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark

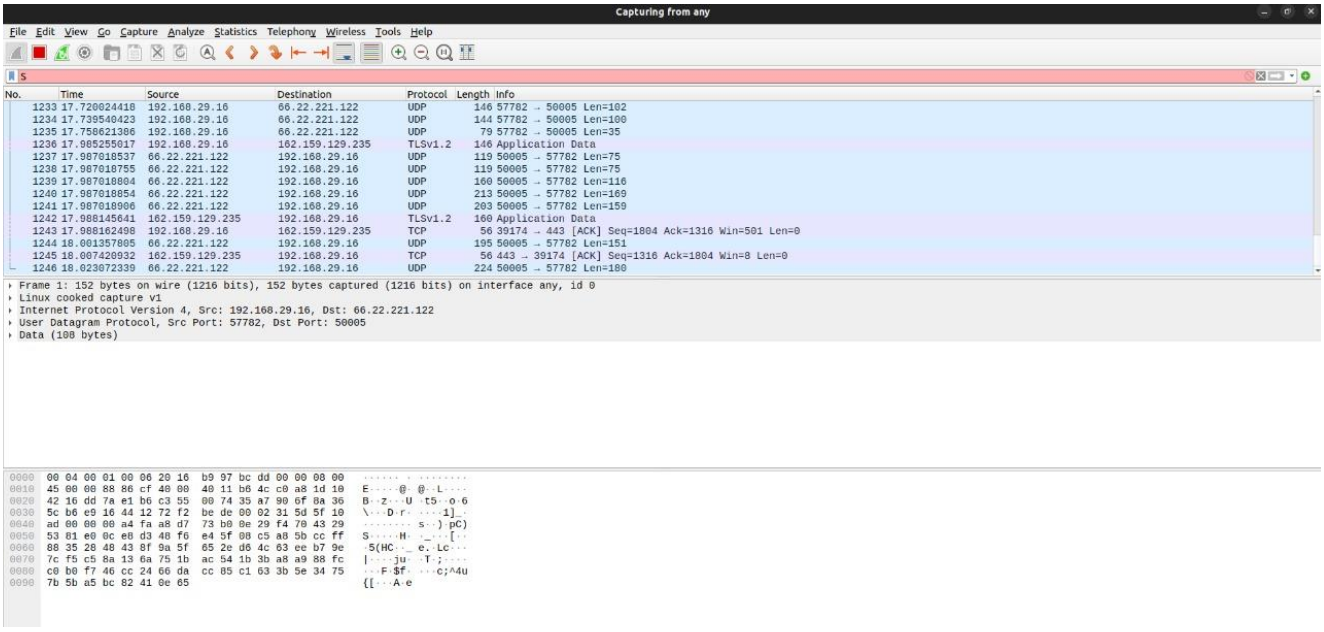
Capture

…using this filter: Enter a capture filter … All interfaces shown

```
wlp7s0
any
Loopback: lo
enp8s0
br-497d2de15195
docker0
bluetooth0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
```

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists


Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

s

```
No.    Time          Source           Destination      Protocol Length Info
  1233 17.720024418  192.168.29.16    66.22.221.122    UDP       146 57782 → 50005 Len=102
  1234 17.739540423  192.168.29.16    66.22.221.122    UDP       144 57782 → 50005 Len=100
  1235 17.758621386  192.168.29.16    66.22.221.122    UDP        79 57782 → 50005 Len=35
  1236 17.985255017  192.168.29.16    162.159.129.235  TLSv1.2   146 Application Data
  1237 17.987018537  66.22.221.122    192.168.29.16    UDP       119 50005 → 57782 Len=75
  1238 17.987018755  66.22.221.122    192.168.29.16    UDP       119 50005 → 57782 Len=75
  1239 17.987018804  66.22.221.122    192.168.29.16    UDP       160 50005 → 57782 Len=116
  1240 17.987018854  66.22.221.122    192.168.29.16    UDP       213 50005 → 57782 Len=169
  1241 17.987018906  66.22.221.122    192.168.29.16    UDP       203 50005 → 57782 Len=159
  1242 17.988145641  162.159.129.235  192.168.29.16    TLSv1.2   160 Application Data
  1243 17.988162498  192.168.29.16    162.159.129.235  TCP        56 39174 → 443 [ACK] Seq=1804 Ack=1316 Win=501 Len=0
  1244 18.001357805  66.22.221.122    192.168.29.16    UDP       195 50005 → 57782 Len=151
  1245 18.007420932  162.159.129.235  192.168.29.16    TCP        56 443 → 39174 [ACK] Seq=1316 Ack=1804 Win=8 Len=0
  1246 18.023072339  66.22.221.122    192.168.29.16    UDP       224 50005 → 57782 Len=180
```

```
› Frame 1: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface any, id 0
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 192.168.29.16, Dst: 66.22.221.122
› User Datagram Protocol, Src Port: 57782, Dst Port: 50005
› Data (108 bytes)
```

```
0000  00 04 00 01 00 06 20 16  b9 97 bc dd 00 00 08 00   ······· ·········
0010  45 00 00 88 86 cf 40 00  40 11 b6 4c c0 a8 1d 10   E·····@· @··L····
0020  42 16 dd 7a e1 b6 c3 55  00 74 35 a7 90 6f 8a 36   B··z···U ·t5··o·6
0030  5c b6 e9 16 44 12 72 f2  be de 00 02 31 5d 5f 10   \···D·r· ····1]_·
0040  ad 00 00 00 a4 fa a8 d7  73 b0 0e 29 f4 70 43 29   ········ s··)·pC)
0050  53 81 e0 0c e8 d3 48 f6  e4 5f 08 c5 a8 5b cc ff   S·····H· ·_···[··
0060  88 35 28 48 43 8f 9a 5f  65 2e d6 4c 63 ee b7 9e   ·5(HC··_ e.·Lc···
0070  7c f5 c5 8a 13 6a 75 1b  ac 54 1b 3b a8 a9 88 fc   |····ju· ·T·;····
0080  c0 b0 f7 46 cc 24 66 da  cc 85 c1 63 3b 5e 34 75   ···F·$f· ···c;^4u
0090  7b 5b a5 bc 82 41 0e 65                            {[···A·e
```

Questions:

1. What is a packet
2. What is packet capture
3. What is filtering in wireshark
4. How can we install wireshark on linux

EXPERIMENT- 8

AIM: Finding out Vulnerable data on Social Networking Sites.

1) **Twitter**

Twitter acknowledged the incident in response to a July HackerOne report that claimed personal information of Twitter users was offered for sale on a dark web marketplace for $30,000. The microblogging company didn’t confirm the number of accounts whose information was collected but sampled some of the on-sale data and verified that a threat actor had indeed exploited the flaw.

Twitter, slapped with a $150 million privacy-related fine in May 2022 and currently in the middle of a takeover pending lawsuit against Elon Musk, said the bug was introduced on the platform in June 2021 and that it had already fixed the vulnerability in January 2022..

2) **Facebook**

A Facebook spokesperson told Insider that the data was scraped due to a vulnerability that the company patched in 2019.While a couple of years old, the leaked data could provide valuable information to cybercriminals who use people's personal information to impersonate them or scam them into handing over login credentials, according to Alon Gal, CTO of cybercrime intelligence firm Hudson Rock, who first discovered the entire trough of leaked data online on Saturday.

"A database of that size containing the private information such as phone numbers of a lot of Facebook's users would certainly lead to bad actors taking advantage of the data to perform social engineering attacks [or] hacking attempts," Gal told Insider.

Gal first discovered the leaked data in January when a user in the same hacking forum advertised an automated bot that could provide phone numbers for hundreds of millions of Facebook users in exchange for a price. Motherboard reported on that bot's existence at the time and verified that the data was legitimate.

.

3) **Gmail**

According to cyber security firm Volexity, the threat research team has found the North Korean 'SharpTongue' group, which appears to be part of, or related to, the Kaimuki advanced persistent threat group, deploying malware called SHARPEXT that doesn't need your Gmail login credentials at all. Instead, it "directly inspects and exfiltrates data" from a Gmail account as the victim browses it. This quickly evolving threat, Volexity says it is already on version 3.0 according to the malware's internal versioning, can steal email from both Gmail and AOL webmail accounts, and works across three browsers: Googlebot +1.2% Chrome, Microsoft’s +1.4% Edge, and a South Korean client called Whale.

4) Instagram

Check Point security researchers have discovered vulnerability on Instagram app, that when exploited by hackers could help them in taking over any victimized account. The Israeli-based firm says thatthe flaw can help the cyber criminals spy on any of the Instagram account by just sending them a malicious image file.

Instagram is a photo and video sharing website and when a sender sends a malicious image through the app, the image file could then allow the hackers to access all messages, images, contacts, camera andlocation data along with the videos on the victim’s phone and can delete them.

Questions:

1. What is identity theft
2. What is cyber stalking
3. What is data breach
4. What are CSRF attacks

EXPERIMENT- 9

AIM: Study of Information Technology Act 2000.

INTRODUCTION

- Information Technology Act 2000, is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
- Information Technology Act 2000 is based on UNCITRAL (United Nations Commission on International Trade Law) Model Law.
- Information Technology Act 2000 has 13 chapters, 94 sections and 4 schedules.

    - The first 14 sections deal with some legal aspects concerning digital signature.
    - Further other sections deal with certifying authorities who are licensed to issue digital signature certificates.
    - Sections 43 to 47 provide for penalties and compensation.
    - Section 65 to 79 of the act deals with offences.
    - Sections 48 to 64 deal with Tribunals and appeal to high court.
    - Section 80 to 94 deals with miscellaneous of the Act.

OBJECTIVES OF THE IT ACT 2000

- This Act may be called the Information Technology Act, 2000.
- It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention there under committed outside India by any person.
- It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.
- Nothing in this Act shall apply to,
    - a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881.
    - a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
    - a trust as defined in section 3 of the Indian Trusts Act, 1882;
    - a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;

- any contract for the sale or conveyance of immovable property or any interest in
- such property; any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

SECTIONS OF IT ACT 2000

List of offences and the corresponding penalties:[7][8]

Section	Offence	Penalty
65	Tampering with computer source documents	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to ₹500,000
66B	Receiving stolen computer or communication device	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	Imprisonment up to three years, or/and with fine up to ₹100,000
66E	Publishing private images of others	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyberterrorism	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to ₹1,000,000
67C	Failure to maintain records	Imprisonment up to three years, or/and with fine.

68	Failure/refusal to comply with orders	Imprisonment up to 2 years, or/and with fine up to ₹100,000
69	Failure/refusal to decrypt data	Imprisonment up to seven yearsand possible fine.
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	Imprisonment up to 2 years, or/and with fine up to ₹100,000
72	Breach of confidentiality and privacy	Imprisonment up to 2 years, or/and with fine up to ₹100,000
72A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years, or/and with fine up to ₹500,000
73	Publishing electronic signature certificate false in certain particulars	Imprisonment up to 2 years, or/and with fine up to ₹100,000
74	Publication for fraudulent purpose	Imprisonment up to 2 years, or/and with fine up to ₹100,000

The offences and the punishments in IT Act 2000:
The offences and the punishments that falls under the IT Act, 2000 are asfollows:-

1. Tampering with computer source documents.
2. Directions of Controller to a subscriber to extend facilities to decryptinformation.
3. Publishing of information which 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 certainparticulars.
7. Penalty for misrepresentation.

8. Confiscation.

9. Power to investigate offences.

10.Protected System.

11.Penalties for confiscation not to interfere with other punishments. 12.Act to apply for offence or contravention committed outside India. 13.Publication for fraud purposes.

14.Power of Controller to give directions.

Questions:

1. Why was IT act necessary to implement
2. What is a cybercrime
3. What is a digital signature
4. Under which section of Indian IT acts were the Chinese apps banned in India.

EXPERIMENT- 10

AIM: Study of HACKING TOOLS

Hacking is the process of using various types of tools or technology in the form of computer programs and scripts to get access to unauthorized data for the security measures of a computer system or network.

Hacking tools and software are nothing but just computer programs or a complex type of script designed by the developers that are used by hackers to know the weaknesses in computer OS, various web applications as well as servers and networks. Nowadays, many employers, especially in the banking sectors, are using ethical hacking tools to secure their data from attackers. Hacking tools are available either in open-source form (freeware or shareware) or in commercial solutions. One can also download such tools from the browser especially if someone wants to use them for malicious purposes.

Ethical hacking tools are used by security professionals specially to get access to computer systems in order to access the vulnerabilities in computer systems so that their security will improve. Security professionals use hacking tools such as packet sniffers to intercept network traffic, password crackers to discover the passwords, port scanners to identify open ports on computers, etc. Though there is a variety of hacking tools available in the market keep in mind what should be its purpose.

Nevertheless, the field of network administration has grown tremendously in the last couple of years. Initially, it is used to simply monitor the networks and now it can be used to manage firewalls, intrusion detection systems (IDS), VPNs, anti-virus software, and anti-spam filters.

Some of the most famous hacking tools in the market are Nmap (Network Mapper), Nessus, Nikto, Kismet, NetStumbler, Acunetix, Netsparker, and Intruder, Nmap, Metasploit, Aircrack-Ng, etc.

IMPORTANCE OF HACKING SOFTWARE

Whenever it comes to hacking software, we often feel anxious or paranoid that it will cause damage to our computer system. However, the reality is so different that employers might need someone as a professional expert to protect the important data concerning valuable assets to companies, hardware, and software systems from attackers. Thus, the need for ethical hacking has become so obvious and important that companies started hiring ethical hackers. Following are some important features of hacking software:

- It provides inside and outside security from the threats to end users.
- It is used to test network security by finding loopholes in it and fixing them.
- One can also download ethical hacking software for his/her home network security from open source and secure it from threats.
- One can also get a vulnerability assessment to protect their network or system from external attacks.

- It is also used to audit the security of the company by ensuring that the computer system is running smoothly with no issues.

SOME TOP ETHICAL HACKING TOOLS –

1) Angry IP Scanner

Angry IP scanner is a lightweight, cross-platform IP address and port scanner. It can scan IP addresses in any range. It can be freely copied and used anywhere. In order to increase the scanning speed, it uses multithreaded approach, wherein a separate scanning thread is created for each scanned IP address.Angry IP Scanner simply pings each IP address to check if it's alive, and then, it resolves its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be saved to TXT, XML, CSV, or IP-Port list files. With help of plugins, Angry IP Scanner can gather any information about scanned IPs.

2) SuperScan

SuperScan is a powerful tool for network administrators to scan TCP ports and resolve hostnames. It has a user-friendly interface that you can use to −

1. Perform ping scans and port scans using any IP range.Scan any port range from a built-in list or any given range.
2. View responses from connected hosts.
3. Modify the port list and port descriptions using the built in editor.
4. Merge port lists to build new ones.
5. Connect to any discovered open port.
6. Assign a custom helper application to any port.

3) Cain & Abel

Cain & Abel is an Operating System password recovery tool provided by Microsoft.

- It is used to recover the MS Access passwords
- It can be used in Sniffing networks
- The password field can be uncovered.
- It Cracks encrypted passwords with the help of dictionary attacks, brute-force, and cryptanalysis attacks.

Price: It is free. One can download it from open source.

4) Nmap (Network Mapper)

Used in port scanning, one of the phases in ethical hacking, is the finest hacking software ever. Primarily a command-line tool, it was then developed for operating systems based on Linux or Unix, and the windows version of Nmap is now available.

Nmap is basically a network security mapper capable of discovering services and hosts on a network, thereby creating a network map. This software offers several features that help in probing computer networks, host discovery as well as detection of operating systems. Being script extensible it provides advanced vulnerability detection and can also adapt to network conditions such as congestion and latency while scanning.

5) Nessus

The next ethical hacking tool on the list is Nessus. Nessus is the world’s most well-known vulnerability scanner, which was designed by tenable network security. It is free and is chiefly recommended for non-enterprise usage. This network-vulnerability scanner efficientlyfinds critical bugs on any given system.

Nessus can detect the following vulnerabilities:

- Unpatched services and misconfiguration
- Weak passwords – default and common
- Various system vulnerabilities

6) Nikto

Nikto is a web scanner that scans and tests several web servers for identifying software that is outdated, dangerous CGIs or files, and other problems. It is capable of performing server-specific as well as generic checks and prints by capturing the received cookies. It is a free, open-source tool, which checks version-specific problems across 270 servers and identifies default programs and files.

Here are some of the chief features of Nikto hacking software:

- Open-source tool
- Checks web servers and identifies over 6400 CGIs or files that are potentially dangerous
- Checks servers for outdated versions as well as version-specific problems
- Checks plug-inns and misconfigured files
- Identifies insecure programs and files

7) Kismet

This is the best ethical hacking tool used for testing wireless networks and hacking of wireless LAN or wardriving. It passively identifies networks and collects packets and detectsnon-beaconing and hidden networks with the help of data traffic.

Kismet is basically a sniffer and wireless-network detector that works with other wireless cards and supports raw-monitoring mode.

Basic features of Kismet hacking software include the following:

- Runs on Linux OS, which may be Ubuntu, backtrack, or more
- Applicable to windows at times

Question :

1) What is Angry IP scanner?
2) What is super scan?
3) What is cain and abel?
4) What is Nmap?