



# VIT<sup>®</sup>

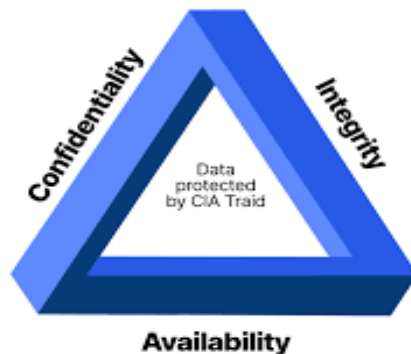
## Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

### J-Component Project

**SUBJECT: Information security analysis and audit  
{CSE3501}**

**NAME OF SCHOOL: School of Computer Science and  
Engineering (SCOPE)**



**PARTICIPANTS: Akshat Sharma – 20BCE2496  
Garv Mittal – 20BCE2857**

**SUBMITTED TO: Murali S Sir.**

## **Introduction:**

**In this document we are going to discuss about the preventions of the attacks that we have implemented in the Review-2.**

## **Abstract:**

**Cybersecurity is the protection to defend internet-connected devices and services from malicious attacks by hackers, spammers, and cybercriminals. The practice is used by companies to protect against phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses.**

**Look around today's world, and we'll see that daily life is more dependent on technology than ever before. The benefits of this trend range from near-instant access to information on the Internet to the modern conveniences provided by smart home automation technology and concepts like the Internet of Things.**

**With so much good coming from technology, it can be hard to believe that potential threats lurk behind every device and platform. A steady rise in cybercrime highlights the flaws in devices and services we've come to depend on. This concern forces us to ask what cyber security is, why it's essential, and what to learn about it and to discuss about the flaws and vulnerabilities, their exploitation and mainly here about the prevention of those exploitations.**

# Arp spoofing

An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices.

And once the attacker succeeds in an ARP spoofing attack, they can

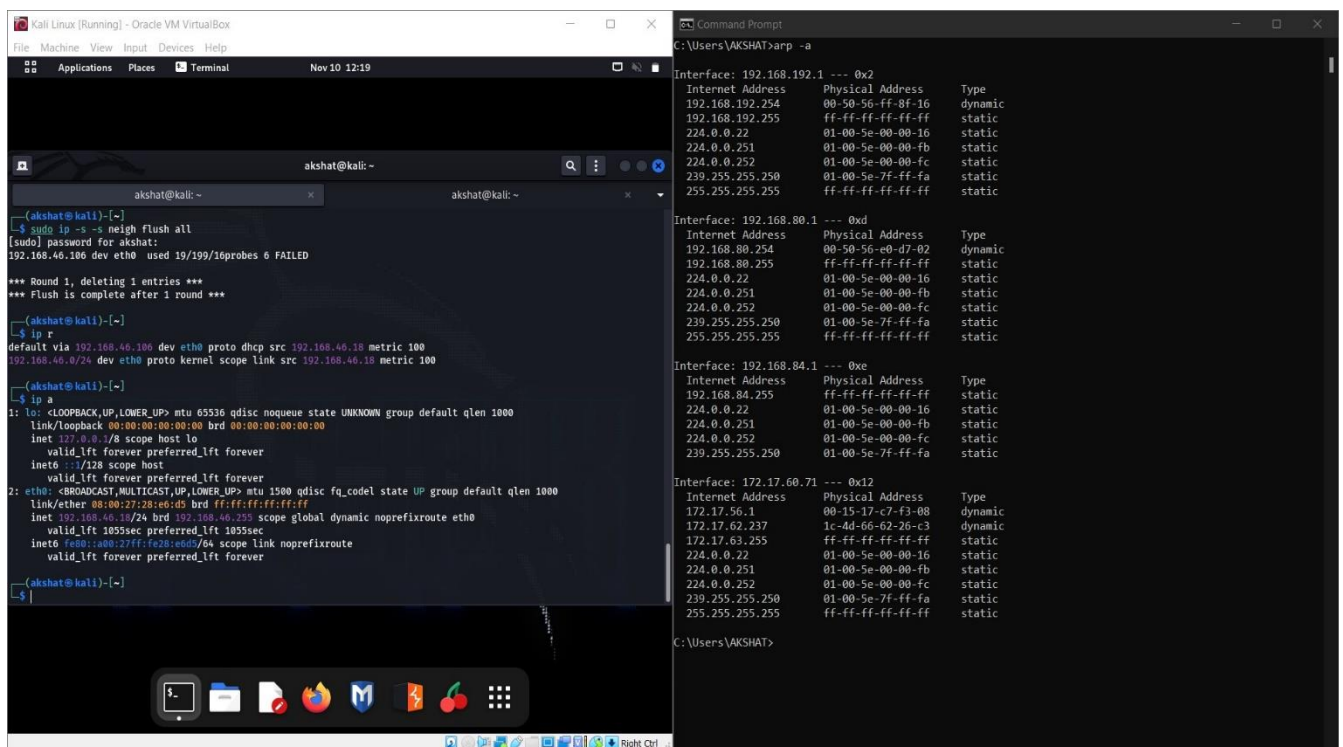
- **Continue routing the communications as-is**—the attacker can sniff the packets and steal data, except if it is transferred over an encrypted channel like HTTPS.
- **Perform session hijacking**—if the attacker obtains a session ID, they can gain access to accounts the user is currently logged into.
- **Alter communication**—for example pushing a malicious file or website to the workstation.

## Preventions

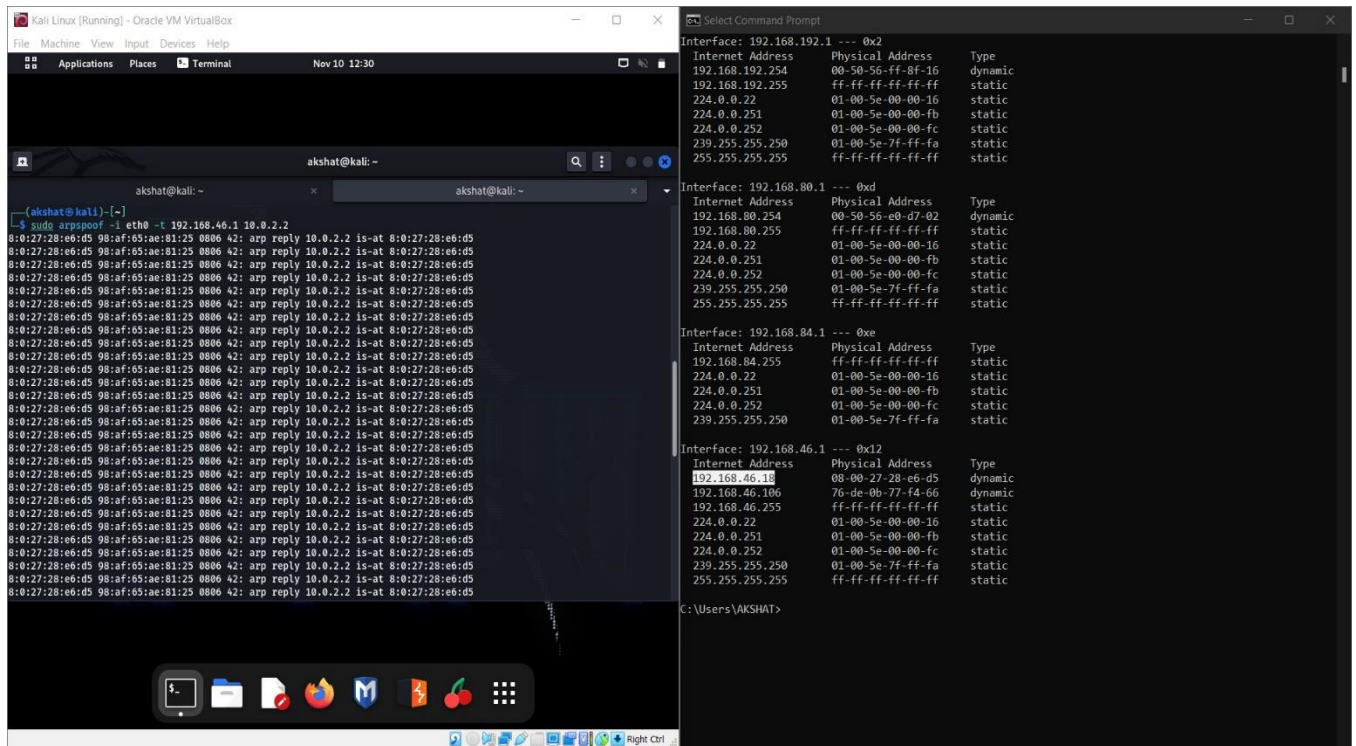
Here are a few best practices that can help you prevent ARP Spoofing on your network:

- **Use a Virtual Private Network (VPN)**—a VPN allows devices to connect to the Internet through an encrypted tunnel. This makes all communication encrypted, and worthless for an ARP spoofing attacker.

### Step-1 – Configuring IP address of our Linux system (192.168.46.18)



## Step-2 – Starting Arp Spoofing



The screenshot shows a Kali Linux virtual machine window on the left and a Windows Command Prompt window on the right. In the Kali terminal, the user has run the command `sudo arpspoof -i eth0 -t 192.168.46.1 10.0.2.2`, which has started a continuous stream of ARP replies to the target IP. The Windows Command Prompt displays the output of the `ipconfig` command for three network interfaces: 192.168.192.1, 192.168.80.1, and 192.168.46.1, showing their respective physical addresses and IP configurations.

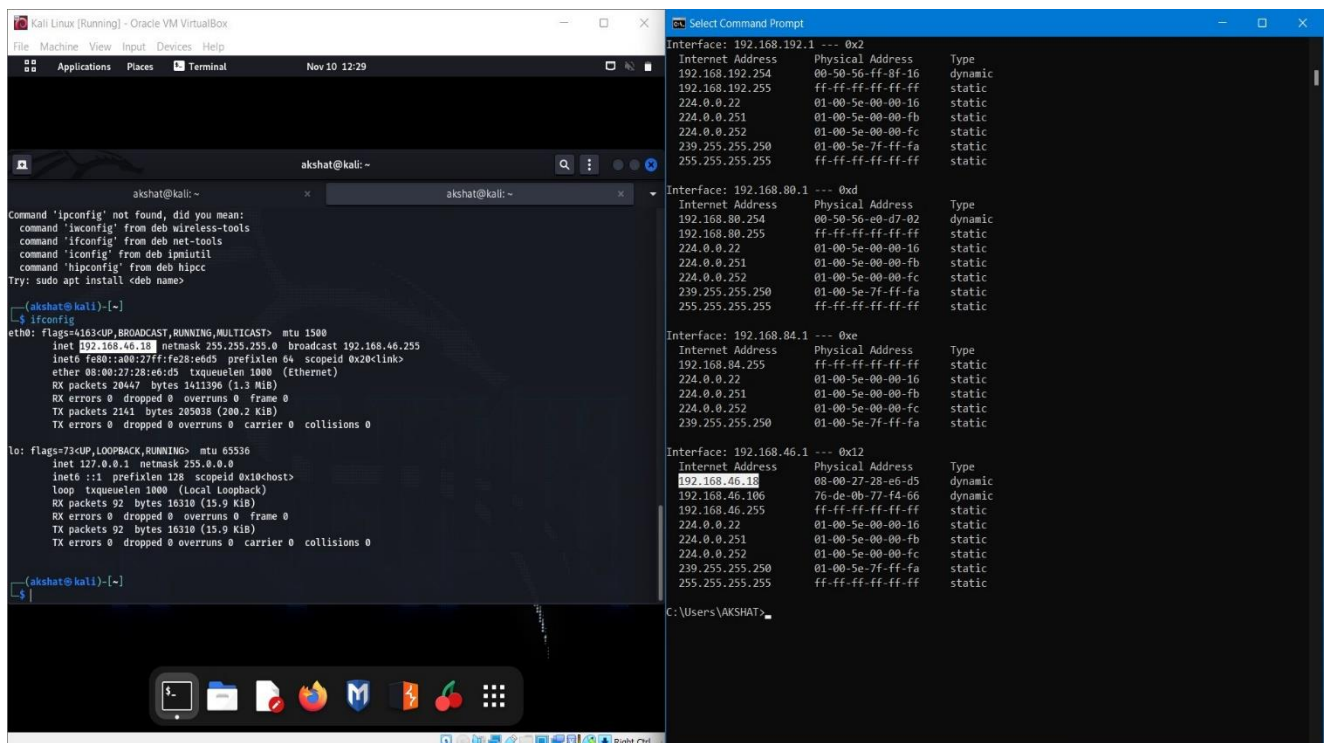
```
Interface: 192.168.192.1 --- 0x2
Internet Address      Physical Address      Type
192.168.192.254       00-50-56-ff-8f-16    dynamic
192.168.192.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.80.1 --- 0xd
Internet Address      Physical Address      Type
192.168.80.254       00-50-56-e0-07-02    dynamic
192.168.80.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.46.1 --- 0x12
Internet Address      Physical Address      Type
192.168.46.10        08-00-27-28-e6-d5    dynamic
192.168.46.106       76-de-0b-77-f4-66    dynamic
192.168.46.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

## Step-3 – Getting Linux IP address on windows CMD terminal (arp -a)

[WHICH MEANS ARP SPOOFING HAS STARTED]



The screenshot shows the same Kali Linux and Windows Command Prompt windows. In the Kali terminal, the user has run the command `ifconfig`, displaying the configuration for the `eth0` interface, including its IP address (192.168.46.10) and MAC address (08:00:27:28:e6:d5). The Windows Command Prompt shows the output of the `arp -a` command, displaying the ARP table for the same three interfaces. The physical addresses listed in the Windows output now match the MAC addresses shown in the Kali terminal, indicating that the ARP spoofing is successful.

```
Interface: 192.168.192.1 --- 0x2
Internet Address      Physical Address      Type
192.168.192.254       00-50-56-ff-8f-16    dynamic
192.168.192.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.80.1 --- 0xd
Internet Address      Physical Address      Type
192.168.80.254       00-50-56-e0-d7-02    dynamic
192.168.80.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.46.1 --- 0x12
Internet Address      Physical Address      Type
192.168.46.10        08-00-27-28-e6-d5    dynamic
192.168.46.106       76-de-0b-77-f4-66    dynamic
192.168.46.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

Step – 4 – Using Wireshark tool to capture all the ARP packets that Linux system is sending

Capturing from Wi-Fi

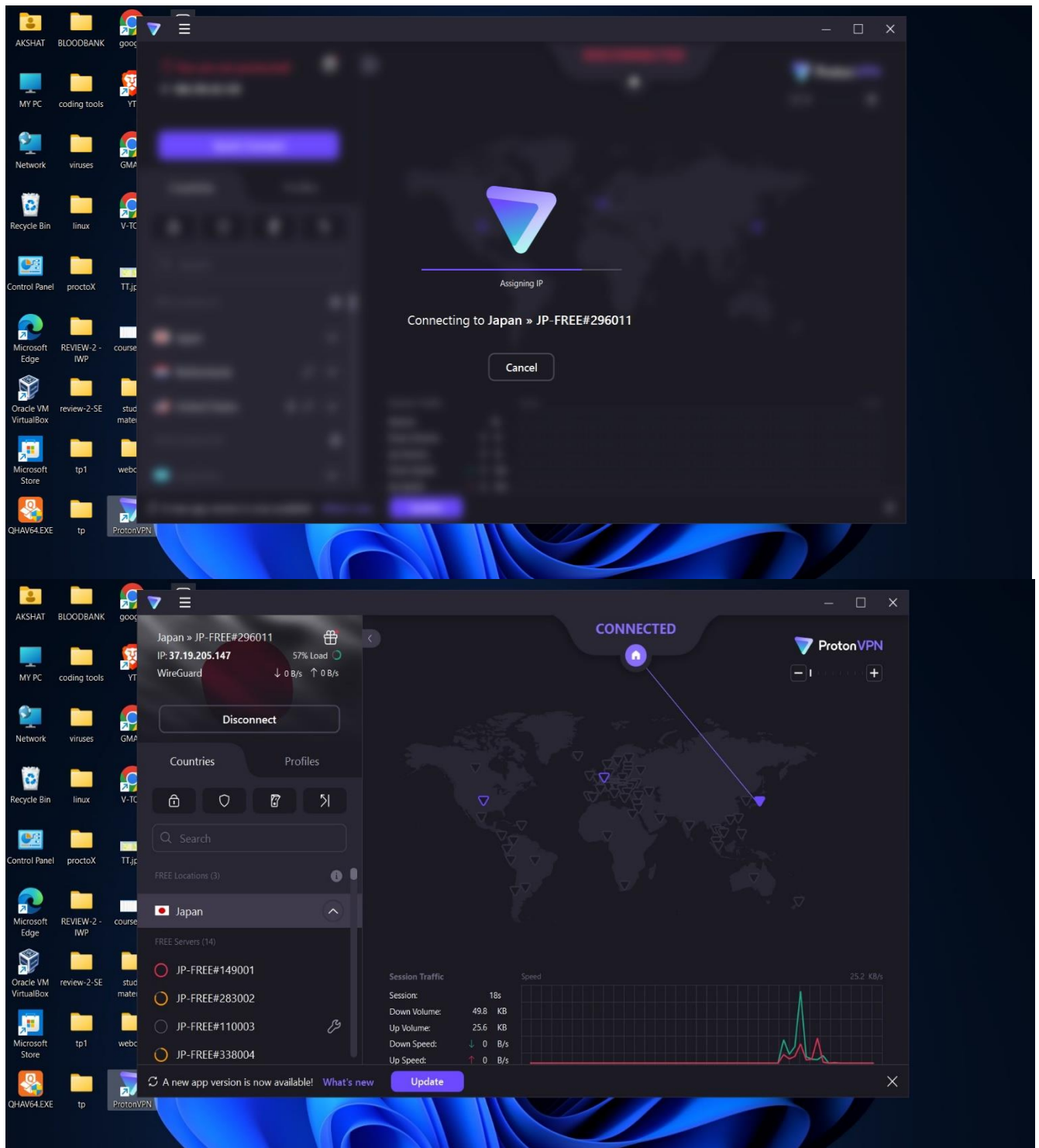
FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

<

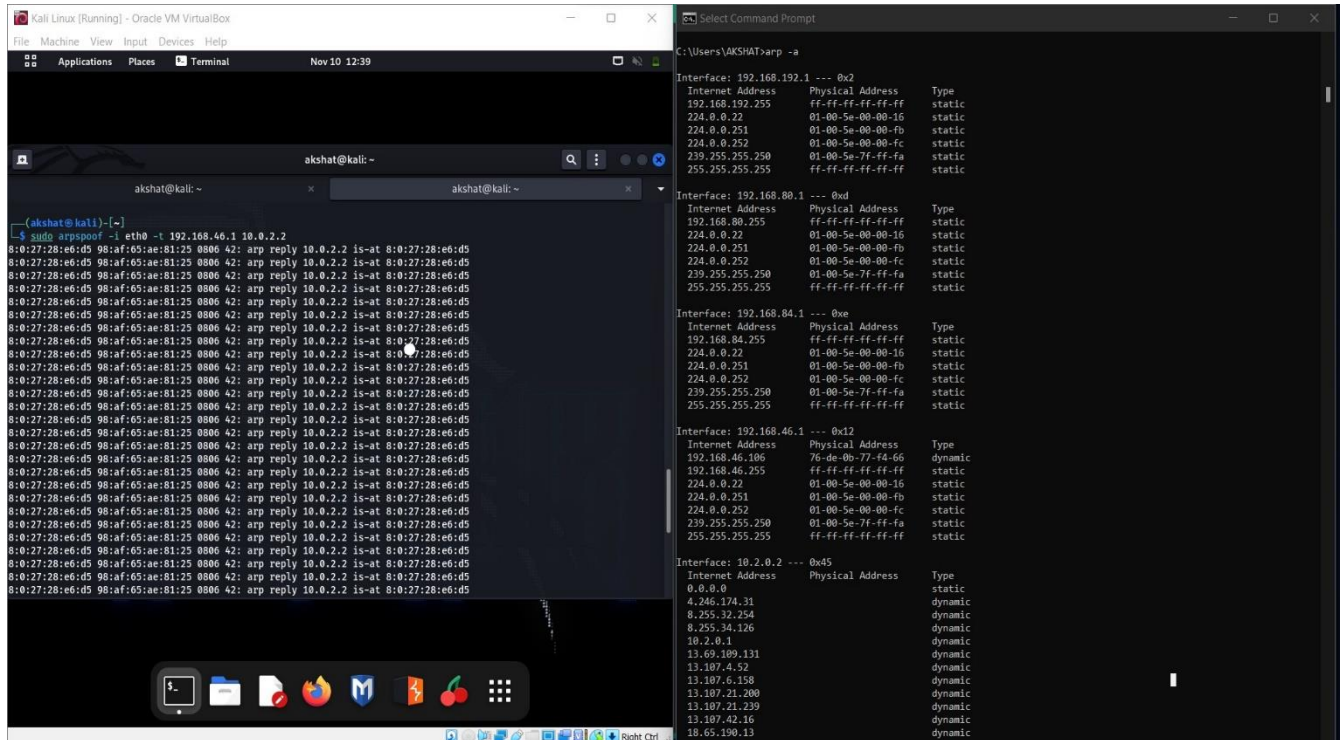


# [STARING PREVENTION]

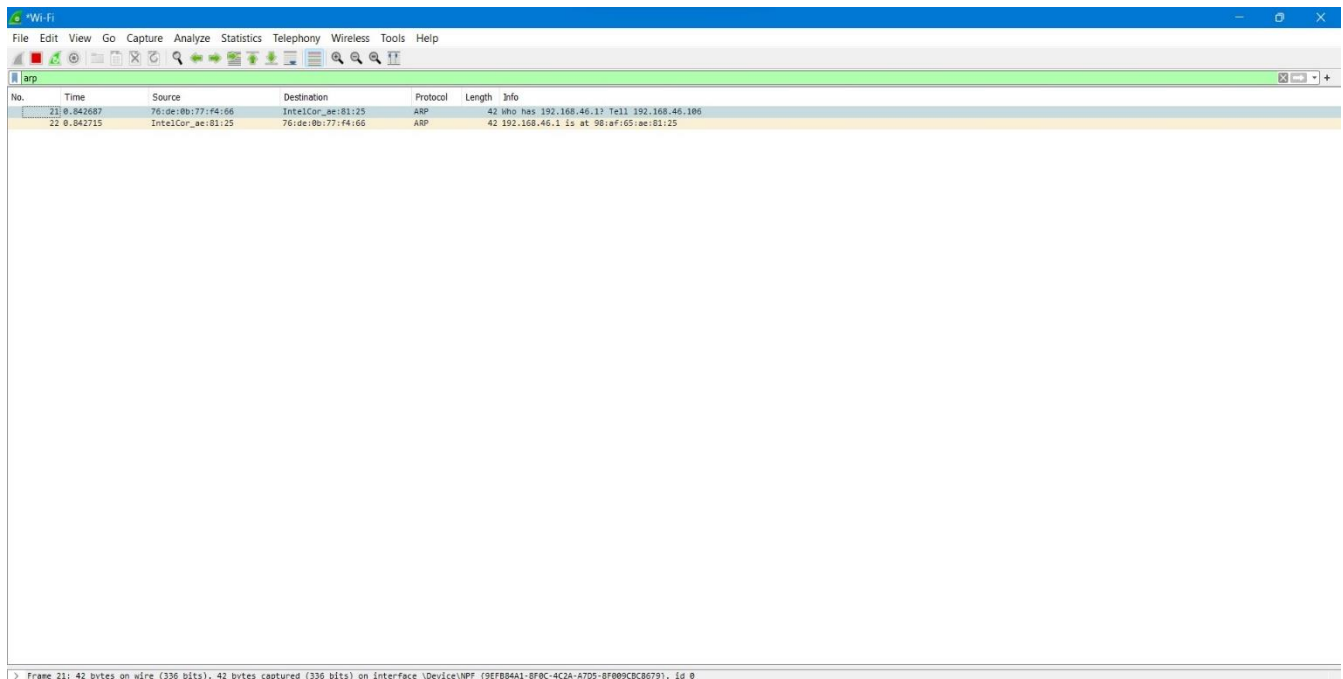
## Step -5- Connecting Windows System to A Virtual Private Network (VPN)



### Step -6 – Again performing ARP spoofing to check if our windows system is still under attack



### Step -7- Noticing that now we are not getting a lot of ARP packets



- **Use static ARP**—the ARP protocol lets you define a static ARP entry for an IP address, and prevent devices from listening on ARP responses for that address. For example, if a workstation always connects to the same router, you can define a static ARP entry for that router, preventing an attack.
- **Use packet filtering**—packet filtering solutions can identify poisoned ARP packets by seeing that they contain conflicting source information, and stop them before they reach devices on your network.
- **Microsegment your endpoints:** One of the best methods of neutralizing the threat of man-in-the-middle attacks is through endpoint security. The µGateway, built by Byos, is a comprehensive endpoint security solution that uses edge microsegmentation to put the user in a protected environment that's isolated from the local network. Known as a "security stack on a stick," µGateway runs a bi-directional firewall, prevents data leakage, and maintains direct and confidential communications with the network gateway without allowing the poisoning of routing tables.
- **Use secure connections:** Although it does not guarantee safety, requiring your employees to only visit sites with an HTTPS connection using secure socket layer (SSL) technology is good practice. All they need to do is make sure the URLs of the sites they go to begin with "HTTPS." While policies are one enforcement strategy, there are also browser plugins that ensure users only visit HTTPS websites.
- **Deploy multi-factor authentication:** This security measure earns its keep when a user's credentials have been compromised. Multi-factor authentication requires users to confirm their identity beyond name and password through an additional route — often a text message. This means that even malicious actors with login credentials will not gain access to your systems.
- **Update your software consistently:** Like educating your employees, this is another security fundamental. But that doesn't make it any less important than the other items on this list. Failing to keep your software up to date creates unnecessary vulnerabilities in your tech infrastructure. So stay on the ball. This due diligence also includes the browsers your organization uses.
- **Employ WPA encryption:** Protect your wireless access points with a robust encryption protocol. Anything less leaves your network susceptible to breach and a subsequent man-in-the-middle attack. So deploy WPA, WPA2, or WPA3 encryption. Preferably WPA3, as it is the strongest of the mechanisms.



# Denial Of Service

A denial-of-service (DoS) attack is a type of cyber-attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to additional users. A DoS attack is characterized by using a single computer to launch the attack.

## Preventions

1. **Perform a network vulnerability audit.** This process includes defining their function within the network, recording the system information, and outlining their existing vulnerabilities. This level of visibility allows you to understand your network's deficiencies, prioritize them by urgency, and patch any holes to keep them from being exploited.
2. **Secure your infrastructure.** To successfully defend against a DoS attack, you need to make sure your castle's walls are fully fortified. For this, it is essential to have multi-level protection strategies that use intrusion prevention and threat management systems. These systems can use anti-spam, content filtering, VPN, firewalls, load balancing, and security layers to spot and block attacks before they overwhelm your network.
3. **Reduce the attack surface.** One of the most effective strategies against DoS attacks is to reduce the size of the available attack area. The smaller the attack surface, the easier it is to defend.

Microsegmentation splits a network into granular zones and protects each zone separately. The net effect is a higher overall security profile. Byos has built a powerful edge microsegmentation solution that uses hardware-enforced isolation to secure endpoints on small microsegments, maximizing the defensive capabilities of the network as a whole

4. **Create a DoS response plan.** . The purpose of the plan is to ensure that your current setup is secure, that you can detect an attack as soon as possible, that everyone on your team knows their role should an attack occur, and that escalation and resolution procedures are all clear.  
This means the plan should provide a systems checklist, define the response team, and lay out the entire response process. In the heat of an attack, it is easy to lose focus and make errors, so have a plan for how to resolve a denial-of-service attack in place to make sure that everyone is ready when the time comes.
5. **Imperva Runtime Application Self Protection (RASP)** complements white box and black box testing by adding an extra layer of protection once the application is already in production or in a realistic staging environment.

# Smurf Attack

A smurf attack is a form of distributed denial-of-service (DDoS) attack that occurs at the network layer. Smurfing attacks are named after the malware DDoS.Smurf, which enables hackers to execute them. More widely, the attacks are named after the cartoon characters The Smurfs because of their ability to take down larger enemies by working together.

## Preventions

A Smurf Attack implies 3 players: the hacker, the intermediary / the amplifier, the victim. In order for the attack to start, the intermediary has to let a source-spoofed IP packet leave its network. Therefore, prevention has to be done on two levels: you must avoid being attacked and you must avoid being used to launch an attack.

To avoid being the amplifier, you should disable IP-directed broadcast on the router – this will make it deny the broadcast traffic to the internal network from other networks. You can also try to apply an outbound filter to your perimeter router, as well as configuring hosts and routers not to respond to ICMP echo requests.

To avoid being the victim

1. traffic network monitoring - have a prevention strategy based on traffic network monitoring that can detect any oddments – like packet volume, behaviour and signature.
2. antivirus and an anti-malware solution  
install an antivirus and an anti-malware solution and protect your servers with network firewalls or specialized web application firewalls.  
Its firewall can help you prevent incoming attacks, while the AV uses 4 stages of scanning (Local File/Signature & Registry Scanning; Real-time Cloud Scanning; Sandbox and Backdoor Inspection; Process Behaviour-based Scanning) to detect and identify even the most advanced threats.
3. Bandwidth - buy more bandwidth. You should have enough bandwidth to handle traffic spikes that might be the result of malicious activity.
4. Redundancy. Your servers should spread across multiple data centres and have a good load balancing system for traffic distribution. The data centres should be, if possible, in different regions of the same country or even in different countries and should be connected to different networks.

5. Protect your DNS servers. Besides building redundancy, you could also try to move to a cloud-based DNS provider, whose services are specifically designed with DDoS prevention in mind.

## Password Hijacking

- It is an attack vector that involves hackers attempting to crack or determine a password. Password hacking uses a variety of programmatic techniques and automation using specialized tools. These password cracking tools may be referred to as 'password crackers'. Credentials can also be stolen via other tactics, such as by memory-scraping malware, and tools like Redline password stealer, which has been part of the attack chain in the recent, high-profile Lapsus\$ ransomware attacks.
- A password can refer to any string of characters or secret to authenticate an authorized user to a resource. Passwords are typically paired with a username or other mechanism to provide proof of identity.
- Credentials are involved in most breaches today. Forrester Research has estimated that compromised privileged credentials are involved in about 80% of breaches. When a compromised account has privileges, the threat actor can easily circumvent other security controls, perform lateral movement, and crack other passwords. This is why highly privileged credentials are the most important of all credentials to protect.
- This in-depth blog highlights password vulnerabilities and risks that give attackers an edge, and provides an overview of password cracking motives, techniques, tools, and defenses.
- Brute Force
- Brute force password attacks utilize a programmatic method to try all possible combinations for a password. This method is efficient for passwords that are short in string (character) length and complexity. This can become infeasible, even for the fastest modern systems, with a password of eight characters or more.
- If a password only has alphabetical characters, including capital letters or lowercase, odds are it would take 8,031,810,176 guesses to crack. This assumes the threat attacker knows the password length and complexity requirements. Other factors include numbers, case sensitivity, and special characters in the localized language.

- With the proper parameters dialed in, a brute force attack will always find the password, eventually. The computing power required and length of time it takes often renders brute force tests a moot by the time it has completed. The time it takes to perform attacks is determined by the time it takes to generate all possible password permutations. Then, the response time of the target system is factored in.
- Brute force password attacks tend to be the least efficient method for hacking a password. Thus, threat actors use them as a last resort.

## Preventions

### 1 Create strong passwords

'password', '123456' or 'abc123' are terrible passwords because they're easy to guess. One way to build a strong password is to think of a phrase or sentence that other people wouldn't know and then use that to build your password.

I have implemented the white list validation so that the user is only allowed to enter a password which is strong enough.

herein I have implemented the same using the RegEx

When a WhiteList violation is detected, the request is changed to the

ProhibCharEncodingException view. WhiteList data validation is disabled by default.

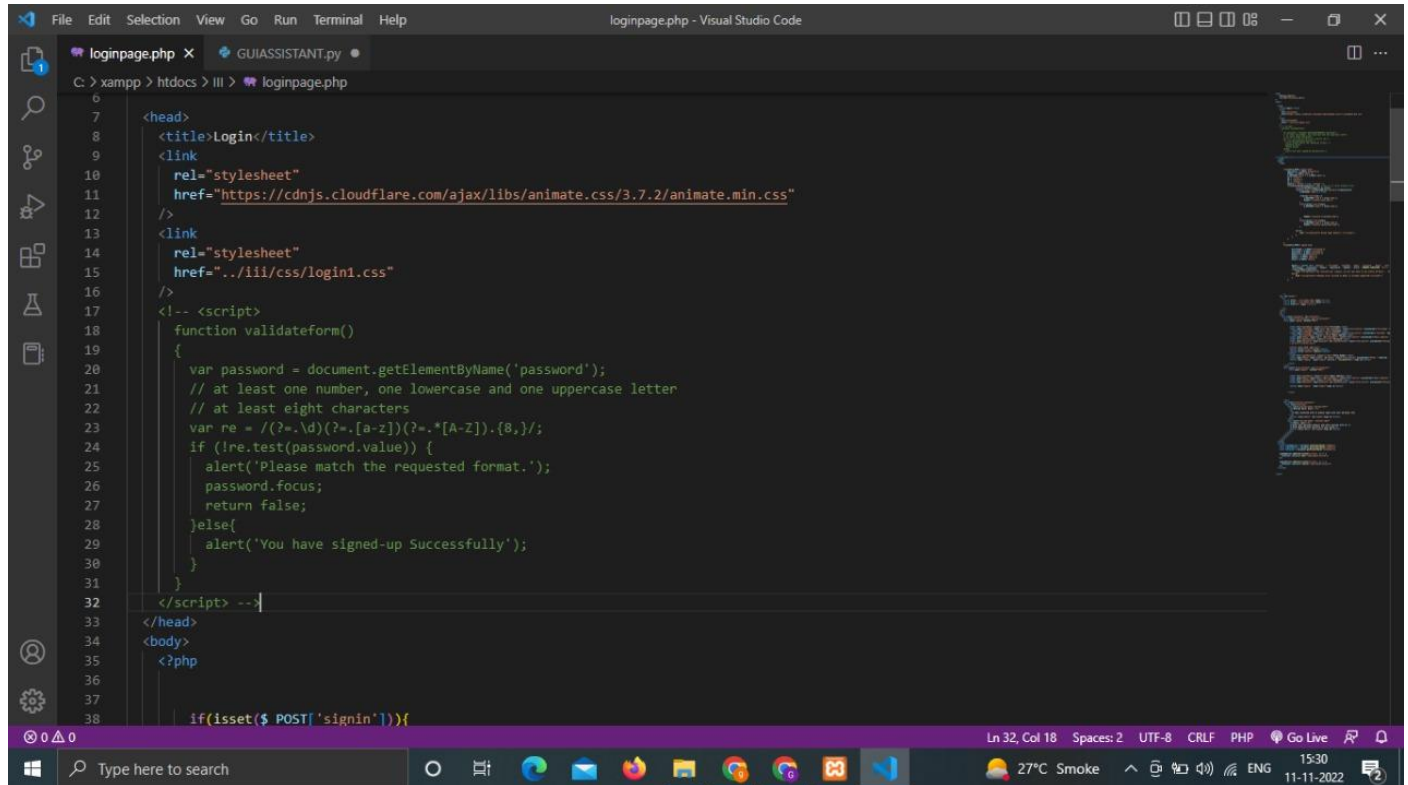
Input validation is your first line of defense when creating a secure application, but it's often done insufficiently, in a place that is easy to bypass, or simply not done at all.

Input validation is the practice of limiting the data that is processed by your application to the subset that you know you can handle. This means going beyond simple data types

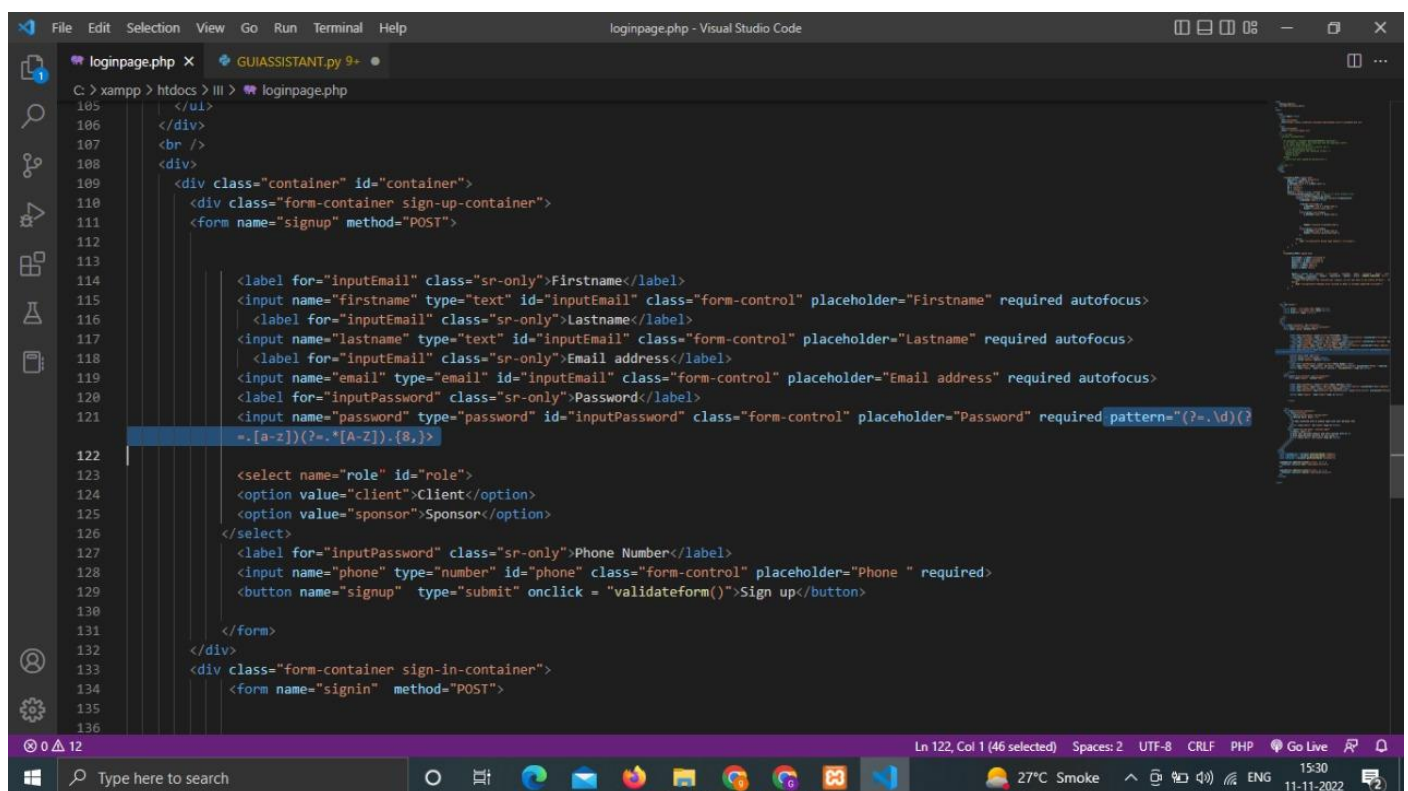
and diving deeply into understanding the ideal data type, range, format and length for each piece of data.

## The Regular Expression

A great way of defining an allowlist for input validation is to leverage Regular Expressions. Regular Expressions are incredibly powerful and useful.



```
loginpage.php
6
7 <head>
8 <title>Login</title>
9
10 <link
11   rel="stylesheet"
12   href="https://cdnjs.cloudflare.com/ajax/libs/animate.css/3.7.2/animate.min.css"
13 />
14 <link
15   rel="stylesheet"
16   href="../../css/login1.css"
17 />
18 <!-- <script>
19   function validateform()
20   {
21     var password = document.getElementById('password');
22     // at least one number, one lowercase and one uppercase letter
23     // at least eight characters
24     var re = /^(?=.*\d)(?=.*[a-z])(?=.*[A-Z]).{8,}/;
25     if (!re.test(password.value)) {
26       alert('Please match the requested format. ');
27       password.focus();
28       return false;
29     }
30     else{
31       alert('You have signed-up Successfully');
32     }
33   }
34 </script> -->
35 </head>
36 <body>
37 <?php
38   if(isset($_POST['signin'])){
```



```
loginpage.php
105 </div>
106 </div>
107 <br />
108 <div>
109 <div class="container" id="container">
110 <div class="form-container sign-up-container">
111 <form name="signup" method="POST">
112
113   <label for="inputEmail" class="sr-only">Firstname</label>
114   <input name="firstname" type="text" id="inputEmail" class="form-control" placeholder="Firstname" required autofocus>
115   <label for="inputEmail" class="sr-only">Lastname</label>
116   <input name="lastname" type="text" id="inputEmail" class="form-control" placeholder="Lastname" required autofocus>
117   <label for="inputEmail" class="sr-only">Email address</label>
118   <input name="email" type="email" id="inputEmail" class="form-control" placeholder="Email address" required autofocus>
119   <label for="inputPassword" class="sr-only">Password</label>
120   <input name="password" type="password" id="inputPassword" class="form-control" placeholder="Password" required pattern="^(?=.*\d)(?=.*[a-z])(?=.*[A-Z]).{8,}/>
121
122   <select name="role" id="role">
123     <option value="client">Client</option>
124     <option value="sponsor">Sponsor</option>
125   </select>
126   <label for="inputPassword" class="sr-only">Phone Number</label>
127   <input name="phone" type="number" id="phone" class="form-control" placeholder="Phone " required>
128   <button name="signup" type="submit" onclick = "validateform()">Sign up</button>
129
130 </form>
131 </div>
132 <div class="form-container sign-in-container">
133 <form name="signin" method="POST">
134
135
136
```



## **2 Secure your passwords**

one should never use the same password across different websites. Some websites allow to add an extra layer of security to your account by enabling a one-time password. Often referred to as an 'OTP', this will require us to enter another 'key' or code to unlock your account in addition to the password. Often referred to as an 'OTP', this will require you to enter another 'key' or code to unlock your account in addition to your password.

## **3 Recall value**

after creating a strong password for each of the online accounts, it can be a challenge to remember them all. So one must consider using a trusted password manager that encrypts and saves your passwords and can be accessed with a single password and an OTP.

## **4. Update your recovery options**

If you do forget your password or get locked out, you need a way to get back into your account. Many services will send an email to you at a recovery email address if you need to reset your password. So it's important to make sure that recovery email address is up-to-date and is linked to an account one can still access.

## **5. Phone-y business**

Sometimes we can also add a phone number to the profile to receive a code to reset your password via SMS. Your mobile phone is a more secure identification method than your recovery email address or a security question because, unlike the other two, you have physical possession of your mobile phone.

## **6. Check your settings**

Social networking sites allow you to share photos, videos, status updates and much more. Many of these services offer privacy settings and controls that help you decide who can see your content before you post it. Use it.

# **Sensitive Data Exposure**

Sensitive data exposure is associated with how teams handle security controls for certain information. Missing or poor encryption is one of the most common vulnerabilities that lead to the exposure of sensitive data. Cybercriminals typically leverage sensitive data exposure to get a hold of passwords, cryptographic keys, tokens, and other information they can use for system compromise. Some commonly known flaws that lead to the exposure of sensitive data include:

- **Lack of SSL/HTTPS Security on Websites** : As web applications gain mainstream use for modern enterprises, it is important to keep users/visitors protected. SSL certificates encrypt data between websites/applications and web servers. Organizations with

misconfigured SSL/HTTPS security risk compromising the users' privacy and data integrity since it can easily be intercepted in transit.

- **SQL Injection Vulnerabilities in Databases :** Without proper security controls, attackers can exploit malicious statements to retrieve the contents of a database. This allows them to create SQL statements that let them perform various database administration actions. Hackers can retrieve sensitive information, such as user credentials or application configuration information, which they use to penetrate further and compromise the system. Without proper security controls, attackers can exploit malicious statements to retrieve the contents of a database. This allows them to create SQL statements that let them perform various database administration actions. Hackers can retrieve sensitive information, such as user credentials or application configuration information, which they use to penetrate further and compromise the system

## Preventions

### How To Prevent 'Sensitive Data Exposure'?

1. Considering the threats you plan to protect this data from (e.g., insider attack, external user), make sure you encrypt all sensitive data at rest and in transit in a manner that defends against these threats.
2. Don't store sensitive data unnecessarily. Discard it as soon as possible. Data you don't have can't be stolen.
3. Ensure strong standard algorithms and strong keys are used, and proper key management is in place.
4. Ensure passwords are stored with an algorithm specifically designed for password protection,
5. Disable autocomplete on forms collecting sensitive data and disable caching for pages that contain sensitive data.
6. Consult Information security experts for detailed and thorough checks of all sensitive web applications.

# Key-logger

Keyloggers are a particularly insidious type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device. The term keylogger, or "keystroke logger," is self-explanatory: Software that logs what you type on your keyboard. However, keyloggers can also enable cybercriminals to eavesdrop on you, watch you on your system camera, or listen over your smartphone's microphone

## Preventions

Keyloggers of poorer quality (such as the malware variety) might reveal themselves in a number of ways. The software might subtly degrade smartphone screenshots to a noticeable degree. On all devices, there could be a slowdown in web browsing performance. Or there's a distinct lag in your mouse movement or keystrokes, or what you are actually typing doesn't show up onscreen. You might even get an error message when loading graphics or web pages. All in all, something just seems "off."

The well-designed commercial grade of keylogger usually works flawlessly, so it does not affect system performance at all. If the keylogger is sending reports to a remote operator, it disguises itself as normal files or traffic. Some of the programs will even display a notice on the screen that the system is being monitored—such as in a corporate computing environment. Others can reinstall themselves if users somehow succeed in finding them and attempt to remove them.

Of course, the best way to protect yourself and your equipment from falling victim to keyloggers is to scan your system regularly with a quality cybersecurity program. For instance, Malwarebytes is fully equipped to sniff out keyloggers. It uses heuristic analysis, signature recognition, and identification of typical keylogger behaviour associated with keystroke and screenshot capturing to first find the malware, and then remove it.

## 5 METHODS TO PREVENT KEYLOGGING ATTACKS

- **Method no. 1 – Use a 2-Step Verification**

Using 2-Step verification helps prevent keylogging attacks. It requires entering a pin code sent to a mobile phone via text to verify identity. It prevents hackers from accessing your account even if he is able to steal your username and password through a keylogger.

If you want to secure your account from unauthorized access, enable a 2-Step verification. When someone tries to access your account without your permission, you'll get notified immediately. That's the primary step on how to prevent keylogging attacks.

- **Method no. 2 – Install Software Updates**

Installing Software updates patches vulnerabilities on the computer. Thus, prevents exploit kits from injecting keyloggers. It addresses the existing issues on the computer that hackers can exploit. It also installs new features on the application, making them more efficient.

Also, remember to install the latest updates for your browsers too. Hackers also exploit outdated plug-ins and add-ons. If you want to keep your computer security tight, install software updates. Installing software updates is another effective method for how to prevent keylogging attacks.

- **Method no. 3 – Use Key Encryption Software**

Key encryption software encrypt the keys you press on the keyboard to prevent keyloggers from capturing the exact keys. They conceal the keystrokes as they reach the application. So keylogger will only be able to log the characters used to encrypt the sensitive information. If you want to add another layer of security against keyloggers, use key encryption software.

- **Method no. 4 – Avoid Downloading Crack Software**

Refusing to download crack software also prevents keyloggers from infecting the computer. Crack software is often infected with malware. They are free, but they could be unsafe for your computer. You may inadvertently install a keylogger disguised as computer software.

If you want to keep your computer malware free, avoid downloading crack software. Download trusted applications only. That's another good way on how to prevent keylogging attacks.

- **Method no. 5 – Install Anti Malware Program**

Anti Malware software protects you from varieties of malware such as keyloggers, ransomware, rootkit and trojan. It scans the files that enter the computer, thus detects and prevents fake software. It also regularly scans the computer for malware to keep the hard drive malware free.

Anti malware software also protects your keyboard from direct access. So it prevents any malicious software from gaining direct access to it.