International Journal of Scientific Research and Engineering Development-– Volume 6 Issue 6, Nov- Dec 2023

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Effective Cloud Security Policy: Best Practices and Case Study

Mohammed. Alnaas[1], Osama. Alhodairy[2], Abduallah. Hanasih[3], Tarek Abbes[4]

[1]*Department of Computer Science, Libyan Academy for Postgraduate Studies, Libya*
info.cs@academy.edu.ly
[2]*National School of Electronics and Telecommunications of Sfax ENETCOM, Tunisia*
osamaalhodairy@gmail.com
[3]*Computer Engineering, Sabratha University, Libya*
ahanashi@sabu.edu.ly
[4]*National School of Electronics and Telecommunications of Sfax ENETCOM, Tunisia*
tarek.abbes@enetcom.usf.tn

--************************----------------------------------

Abstract:

The main purpose of cloud cryptography is to protect sensitive data without causing any delay in data transfer, various cryptographic protocols designed to balance data security and performance to secure data through encryption. One such approach is to encrypt the data before uploading it to the cloud.

This study proposes an effective framework for protecting small and medium companies (SMEs) from cybersecurity risks and threats. The framework evaluates the system of private encryption data in a server environment using the advanced encryption standard (AES) 128 algorithm and a virtual private network (VPN) tunnel. The goal is to secure data through encryption and ensure data transfer without causing delays. The framework includes a test case where data is transferred from a storage area network (SAN) storage to the cloud. To assess the system's performance and security, a penetration test using Kali Linux is conducted. The results of this study provide insights into securing SMEs' data and mitigating cybersecurity risks effectively.

Keywords**—** ERM, RMF, Cloud Security, AES Algorithm, Kali Linux, BPDU, DEP.

I. INTRODUCTION

Cyber terrorism and cyber financial fraud are considered to be two standards of concern for most countries. According to the internet crime report (IC3) [1, 2], in 2020, the United States federal bureau of investigation (FBI) received more than 467,000 cybercrime complaints that caused an estimated US$3.5 billion in losses as illustrated in Fig1.

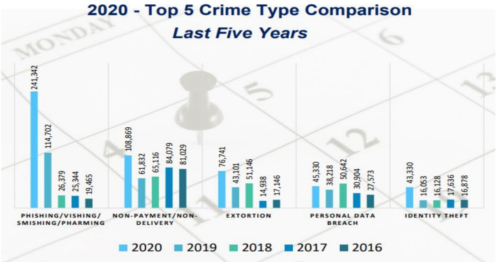


Fig 1: Victim Loss Comparison Reported Crime Types in 2020

Accordingly, many governments have provided protective measures, believed that small companies were not recognized as potential targets of cyber-attacks. However, attention paid to the governments' bodies, large companies and individuals citizens [3, 4].

Accordingly, many governments have provided protective measures, believed that small companies were not recognized as potential targets of cyber-attacks. However, attention paid to the governments' bodies, large companies and individuals citizens [3, 4].

Cloud security is essential in safeguarding internet-connected systems, including hardware, software, and data, against cyber-attacks. Given the complexity and uncertainty of modern technologies, understanding the risks and implications of each interaction within computer systems is challenging [5].

However, it is crucial to recognize that every point of contact leaves traces that can have significant security implications.

A comprehensive cloud security policy encompasses multiple aspects, including data protection, regulatory compliance, customer privacy, and authentication rules for users and devices. By configuring security measures tailored to specific business needs, organizations can authenticate access, filter traffic, and ensure the security of their cloud environments [6].

Cloud cryptography plays a crucial role in securing sensitive data during transfer without introducing significant delays. Various cryptographic protocols have been developed to strike a balance between data security and performance. One approach involves encrypting data before uploading it to the cloud, ensuring that it remains secure throughout its lifecycle [7].

To address the security needs of SMEs, this study proposes an effective framework that considers the specific challenges faced by these organizations. The framework includes the use of the AES 128 algorithm and a VPN tunnel to protect data during its transmission from SAN storage to the cloud. By employing these security measures, SMEs can mitigate the risks associated with data breaches and unauthorized access.

To evaluate the effectiveness of the proposed system, a penetration test is conducted using Kali Linux. This test simulates real-world attacks to assess the system's vulnerability and identify potential weaknesses. By measuring and evaluating the system's performance under these conditions, organizations can gain insights into its effectiveness and make necessary improvements to enhance their overall security posture.

II. Enterprise Risk Management (ERM)

ERM is a framework affected by the board of directors and the management of an entity, it aims to identify potential events that may affect the entity and to manage risks using its risk appetite as illustrated in Fig 2.

Risk appetite is the level of risk that the entity is prepared to accept in pursuit of its objectives [9, 10]. ERM offers assurance regarding the accomplishment of objectives set by the entity.

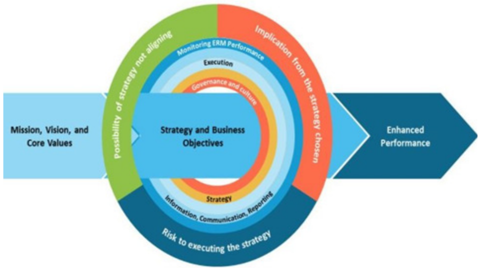

Mission, Vision, and Core Values
Possibility of strategy not aligning
Monitoring ERM Performance
Execution
Governance and culture
Strategy and Business Objectives
Strategy
Information, Communication, Reporting
Implication from the strategy chosen
Risk to executing the strategy
Enhanced Performance

Fig 2: Enterprise Risk Management

In ERM, uncertainty has both risk and opportunity. Risk can reduce value while an opportunity can enhance value. ERM components described as follows:

1. Internal environment: the internal environment provides basics on how risk and control addressed.
2. Objective setting: before the management identifies potential events, objectives of the entity are set. ERM makes sure that the objectives are consistent with the risk appetite.
3. Event identification: potential events affecting the entity identified. This process involves identification of events from internal or external sources, which affect the accomplishment of objectives.
4. Risk assessment: identified risks analysed and assessed on both inherent and residual basis considering risk likelihood and impact.
5. Risk response: possible responses to risks identified. They include avoiding, accepting, reducing, and sharing risks.
6. Control activities: policies, procedures, and controls are established and implemented to sustain the risk response decisions.
7. Information and communication: relevant information captured and communicated enabling people to carry out their responsibilities.
8. Monitoring: ERM entirely monitored to react dynamically as changes made.

III. Cyber Security Risk Management Frameworks (RMF)

Risk management is the process of identifying potential risks, assessing the impact of those risks, and planning how to respond if the risks become reality. Cyber risk management is the practice of prioritizing cybersecurity defensive measures based on the potential adverse impact of the threats they are design to address, it referred to as a series of activities of controlling risk within its acceptable level.

However, cyber security management involves a series of decision-making processes to select, implement, and maintain the proper controls. Security threats change over time and supportive resources are limited [9].

Establishing a risk management approach to cybersecurity investment acknowledges that no organization can completely eliminate every system vulnerability or block every cyber-attack.

Cyber risk management frameworks present standardized and well-documented methodology for the following:

1. Conducting risk assessments that evaluate business priorities and identify gaps in cybersecurity controls
2. Performing risk analysis on existing control gaps
3. Prioritizing future cybersecurity investment based on risk analysis
4. Executing on those strategies by implementing a range of security controls and best practices
5. Measuring and scoring cybersecurity program maturity along the way

The national institute of standards and technology (NIST) risk management framework provides a process that integrates security, privacy, and cyber supply-chain risk management activities into the system development life cycle [8].

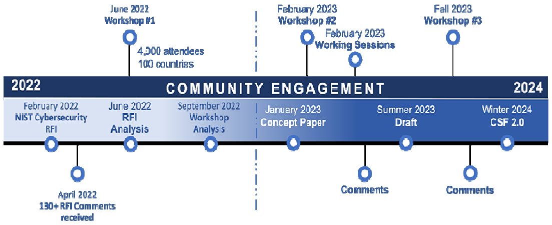


Fig 3. NIST cybersecurity framework

The RMF approach can be applied to new and legacy systems, any type of system or technology (e.g., IoT, control systems), and within any type of organization regardless of size or sector

The NIST cybersecurity framework as illustrated in Fig 3 called for greater collaboration between the public and private sector for identifying, assessing, and managing cyber risk. While compliance is voluntary, NIST has become the gold standard for assessing cybersecurity maturity, identifying security gaps, and meeting cybersecurity regulations.

In February 2022, NIST issued a public request for information (RFI) seeking feedback and suggestions on how to improve their existing framework. As a result of the RFI and subsequent analysis and workshops, the NIST cybersecurity framework is undergoing its biggest update [10].

IV. Cloud Security

Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data, and infrastructure. These security measures configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices [14].

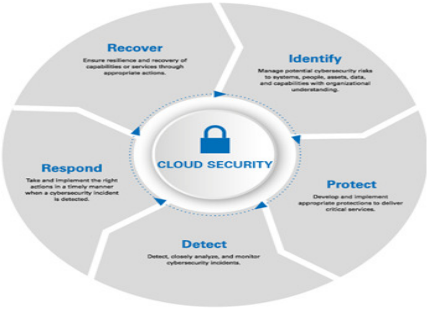

Recover
Ensure resilience and recovery of capabilities or services through appropriate actions.
Identify
Manage potential cybersecurity risks to systems, people, assets, data, and capabilities with organizational understanding.
CLOUD SECURITY
Respond
Take and implement the right actions in a timely manner when a cybersecurity incident is detected.
Protect
Develop and implement appropriate protections to deliver critical services.
Detect
Detect, closely analyze, and monitor cybersecurity incidents.

Fig 4. Cloud Security Cycle

From authenticating access to filtering traffic, cloud security configured to the exact needs of the business, because these rules can be configured and managed in one place, administrations overheads are reduced, and IT teams empowered to focus on other areas of the business.

The way cloud security delivered will depend on the individual cloud provider or the cloud security solutions in place, but implementation of cloud security processes should be a joint responsibility between the business owner and solution provider [15].

The advantages of cloud computing over traditional networks are well known and they include fast deployment as illustrated in Fig 4.

However, identification of the risks in cloud computing is more difficult, because of the lack of a dedicated framework. Such risks make businesses feel difficulty when adopting cloud technology. Many documents written about risks and guidelines regarding the cloud computing adoption.

These documents rank highly as a security concern, but rank low across risks where a dedicated risk management framework is required [16].

V. Case Study

HQCS is a small virtual company that contains around 40 employees, which pass to enter the building and have company pcs. The network system built and introduce its construction as illustrated in Fig 5.

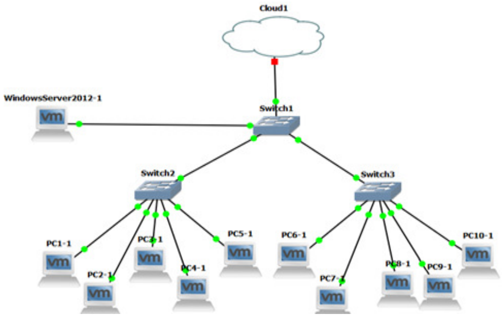


Fig 5. Connection of the Network Parts

The configuration of the network that specifies the parts is shown in Table I, where the network construction based on one virtual local area network (VLAN) divided into two subnets, the first one (192.168.2.0/24) for computers in all company's departments, and the second subnet (192.168.3.0/24) for the server management and switches IP management.

Table I. Network configuration

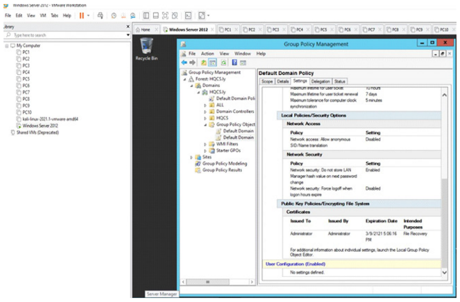
Firewall Configuration	Inside IP 10.10.10.1/30 Outside IP (Public IP) 50.50.50.50 255.255.255.250
Core Switch Config	Port 1 (p-t-p) with FW (10.10.10.2/30 SRV (Vlan 3) 192.168.3.0/24 Users (Vlan2) 192.168.2./24
Access Switches Management	SW1 192.168.2.253/24 SW2 192.168.3.253/24
SRV IP	192.168.3.12
DC PHY(AD role)	(192.168.3.12 255.255.255.0)
Client Vlans	To be created on Core Switch Vlan 2 (192.168.2.1…200/24)

Devices were connected through a number of two network switches with, specifications of the operating system (OS) and windows servers 2012. Active directory (AD) server has been added to control the permissions of the devices as specifications illustrated in the Table II.

TABLE II. OS SPECIFICATIONS

Servers	Active Directory (AD)
Client	All Client Machine based on OS windows 10 Enterprise
Firewall	Cisco Switches (5525)
Access Switches	Cisco Switches (9300)
Core Switches	Cisco Switches (9500)
Kali Linux	Distributor ID: Kali Description: Kali GNU/Linux Rolling Release: 2021.1 Codename: kali-rolling
VMware	Workstation 16 Pro 16.1.1 build-17801498
GNS 3	GNS 3 2.2.19 Under GPL v3 license
Microsoft Visio Drawing	Microsoft Visio professional 2013 license

A default group policy management is automatically created and linked to the domain, which is generally used to manage default account settings, it represents the default policy that applied to all domain controllers in the domain controller container as described in Fig 6.



Default Domain Policy

Policy	Setting
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Security Options

Network Access

Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled

Network Security

Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled

Public Key Policies/Encrypting File System

Certificates

Issued To	Issued By	Expiration Date	Intended Purposes
Administrator	Administrator	3/9/2121 5:06:16 PM	File Recovery

For additional information about individual settings, launch the Local Group Policy Object Editor.

User Configuration (Enabled)

No settings defined.

Fig 6. Default Group Police Management with AD

AD users and computers are a Microsoft management console, through which centralized management of objects like computers, users, and groups in AD.

It used for performing create, manage, edit and delete users, groups, and computer accounts, that allows to create a tree similar to our organization's structure using organizational units (OU), which is similar to a container, that can place users, computers, groups, and other OU.

VI. PROPOSAL CYBER SECURITY IN CLOUD DATA COMBINED WITH ENCRYPTION METHODOLOGY

A strategic cyber security in cloud data combined with encryption methodology defense solution is required to address the multifaceted security concerns from mobile to connected devices utilizing the cloud, as well as the underlying screening of information technology (IT) analytics.

These procedures protect the system from cyber-attack by activating the main protection features of AD and network switches [17, 18].

In addition, a suggestion of an encryption and masking system to protect data before it is uploaded to the cloud.

A. AD Security

AD policies for windows server 2012 is a central identity store, authentication provider to system working as a domain controller as described in Fig 7.

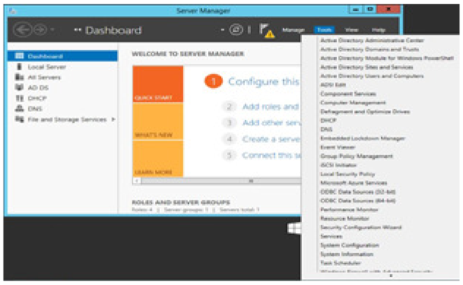


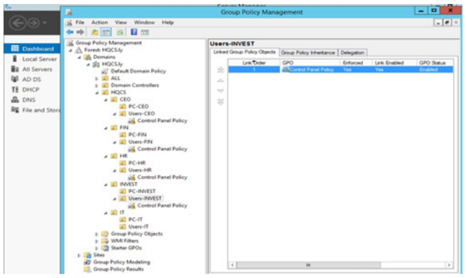
Fig 7. Active Directory (AD)

It authenticates, authorizes all users and computers in a windows domain type network, assigning and enforcing security policies for all computers, restrict installing or updating software as illustrated in Fig8. Furthermore, it prevents windows from storing LAN manager Hash and disallow removable media drives, DVDs, CDs, and Floppy Drives. Furthermore, it is responsible for setting the minimum password length to higher limits [19].

B. Moderating Access to Control Panel

Setting limits on a computers' control panel creates a safer business environment. Therefore, moderating who has access to the computer, user can keep data and other resources safe.

In this stage of using the group policy management editor for the OU, user configuration, policies, administrative templates, control panel and setting call access to control panel and PC setting, must closing all the windows control panel, except for IT (for use in providing technical support) as described in Fig 8.



Users-INVEST

Link Order	GPO	Enforced	Link Enabled	GPO Status
1	Control Panel Policy	Yes	Yes	Enabled

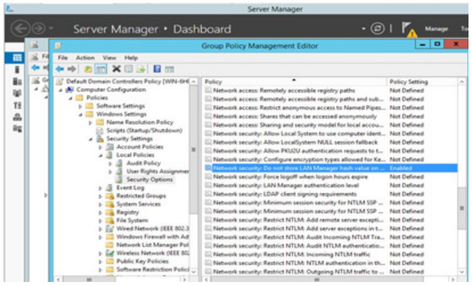
Fig 8. Apply Policy for all OU Except IT

Note that, when it is used on the level of users, it is linked to the user only and has nothing to do with the device.

C. Avoid Windows Storing LAN Manager Hash

Windows generates and stores user account passwords in hashes. It generates both a LAN manager hash (LM hash) and windows NT hash (NT hash) of passwords. It stores them in the local security accounts manager (SAM) database or active directory.

The LM hash is weak and disposed to to hacking. Therefore, prevent windows from storing an LM hash of the user's passwords as shown in Fig 9.



Policy	Policy Setting
Network access: Remotely accessible registry paths	Not Defined
Network access: Remotely accessible registry paths and sub...	Not Defined
Network access: Restrict anonymous access to Named Pipes...	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accou...	Not Defined
Network security: Allow Local System to use computer ident...	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to t...	Not Defined
Network security: Configure encryption types allowed for Ke...	Not Defined
Network security: Do not store LAN Manager hash value on ...	Enabled
Network security: Force logoff when logon hours expire	Not Defined
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Not Defined
Network security: Minimum session security for NTLM SSP ...	Not Defined
Network security: Minimum session security for NTLM SSP ...	Not Defined
Network security: Restrict NTLM: Add remote server excepti...	Not Defined
Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Tra...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in th...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to ...	Not Defined

Fig 9. Prevent Windows Storing LAN Manager Hash Enabled

D. *Control Access to Command Prompt*

Command prompts can be used to run commands that give high-level access to users and avoid other restrictions on the system. Therefore, to ensure system resources' security, disable command prompt.

If someone tries to open a command window, the system will display a message stating that settings are preventing this action.

E. *Disallow Removable Media Drives, DVDs, CDs, and Floppy Drives*

Removable media drives very likely to infection. They may contain a virus or malware. If a user plugs an infected drive into a network computer, it can affect the entire network.

Therefore, disable all these drives entirely [20, 21].

Specify the access permission for the user, not the computer configuration, that is including deny the user configuration from read and write access for CD, DVD and Floppy driver, also, for Tape driver and WPD devices.

F. *Apply Software Restriction Policies*

Choice of software installation may install unwanted apps that compromise the system. System admins routinely do maintenance and cleaning of such systems. Prevent software installations through group policy to keep it as safe as possible.

G. *Disable Guest Account*

Users can get access to sensitive data through a guest account, grant access to OS, because it does not require a password [22]. Enabling this kind of account means anyone can misuse and abuse access to the systems, disabled these accounts by default to prevent people from abusing access.

H. *Set Minimum Password Length to Higher Limits*

For domain accounts, the setting of the system been updated to be the minimum password length to be at least 12 characters, setting lower value for minimum password length creates unnecessary risk, the maximum password age chosen to be 23 days (this is nothing, but almost one working month).

Moreover, the property store password using reversible encryption been disabled.

I. *Disable Anonymous Security Identifiers (SID) Enumeration*

In windows OS any one may query the SIDs to identify important users and groups, this facility can exploit by the hackers to get unauthorized access to data, by default, this setting disabled and ensure that it remains that way [19, 23].

VII. CORE SWITCH

A core switch (tandem switch or a backbone switch) is a high-capacity switch generally positioned within the backbone or physical core of a network. It serves as the gateway to a wide area network (WAN) or the Internet. Core switch provide the final aggregation point for the network and allow multiple aggregation modules to work together.

The upgraded system requires to configure out a VLAN for each department, and therefore IT professional technical can manage (prevent. allow) communication between VLANs, core switch and then claim as needed as illustrated in Table III.

TABLE III. NETWORK CONFIGURATION OF STUDY CASE AFTER UPGRADING THE SYSTEM

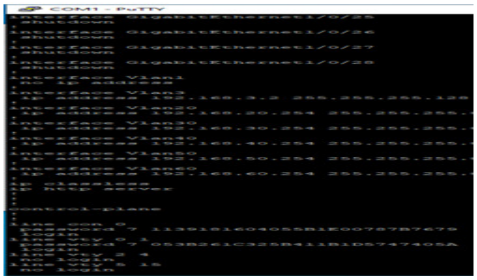
Firewall Config	Inside IP 10.10.10.1/30 Outside IP (Public IP) 50.50.50.50 255.255.255.250
Core Switch Config	Port 1 (p-t-p) with FW (10.10.10.2/30) SRV Vlan (Vlan 3) 192.168.3.0/24 **Users Vlan {Vlan 20** (192.168.20.0/24) **Vlan 30** (192.168.30.0.24) **Vlan 40** (192.168.40.0/24) **Vlan 50** (192.168.50.0/24) **Vlan 60** (192.168.60.0/24)}
Access Switches Management	SW1 192.168.2.253/24 SW2 192.168.3.253/24
SRV Vlans	192.168.3.12
DC PHY(AD role)	(192.168.3.12 255.255.255.0)
Client Vlans	To be created on Core Switch **Vlan 20** (192.168.20.0/24) **Vlan 30** (192.168.30.0.24) **Vlan 40** (192.168.40.0/24) **Vlan 50** (192.168.50.0/24) **Vlan 60** (192.168.60.0/24)

A. *Enable & Encrypt Secret Password*

In order to grant privileged administrative access to the device, user should create a strong (enable secret) password, the system use a password with 12 characters long consisting of alphanumeric and special symbols as well as command, which creates a password with strong encryption.

All the passwords configured on the cisco device (except the enable secret) shown as clear text in the configuration file.

In order to encrypt the clear text passwords and obscure them from showing in the configuration file, the global command (service password-encryption) used here as illustrated in Fig 10.



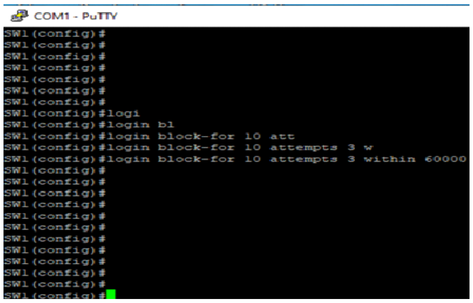
```
interface GigabitEthernet1/0/25
 shutdown
!
interface GigabitEthernet1/0/26
 shutdown
!
interface GigabitEthernet1/0/27
 shutdown
!
interface GigabitEthernet1/0/28
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan3
 ip address 192.168.3.2 255.255.255.128
!
interface Vlan20
 ip address 192.168.20.254 255.255.255.
!
interface Vlan30
 ip address 192.168.30.254 255.255.255.
!
interface Vlan40
 ip address 192.168.40.254 255.255.255.
!
interface Vlan50
 ip address 192.168.50.254 255.255.255.
!
interface Vlan60
 ip address 192.168.60.254 255.255.255.
!
ip classless
ip http server
!
!
control-plane
!
!
line con 0
 password 7 1139181604055B1E00787B7679
 login
line vty 0 1
 password 7 0538261C325B411B1D5747405A
 login
line vty 2 4
 no login
line vty 5 15
 no login
```

Fig 10. Enable and Encrypt Password

B. *Configure Maximum Failed Authentication Attempts*

To avoid brute force password attacks to the devices, the system configures maximum number of failed login attempts, so that a user will locked out after this threshold [21].

Login block feature allows users to enhance the security of a router by configuring options to automatically block further login attempts when a possible denial-of-service (DoS) attack is detected as illustrated in Fig 11.

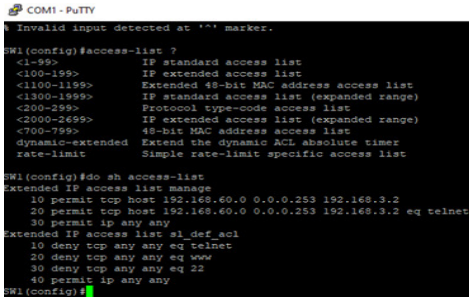


```
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#logi
SW1(config)#login bl
SW1(config)#login block-for 10 att
SW1(config)#login block-for 10 attempts 3 w
SW1(config)#login block-for 10 attempts 3 within 60000
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
```

Fig 11. Login Enhancements

C. *Restrict Management Access to Specific IPs only*

This is probably one of the most important security configurations on cisco network devices. The system restrict what IP addresses can Telnet or SSH to the devices. This should be limited to a few management systems that administrators will be using to manage the network. In this case, only allow to IT VLAN as described in Fig 12.



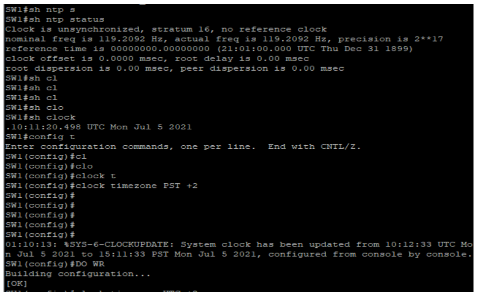
```
% Invalid input detected at '^' marker.

SW1(config)#access-list ?
  <1-99>             IP standard access list
  <100-199>          IP extended access list
  <1100-1199>        Extended 48-bit MAC address access list
  <1300-1999>        IP standard access list (expanded range)
  <200-299>          Protocol type-code access list
  <2000-2699>        IP extended access list (expanded range)
  <700-799>          48-bit MAC address access list
  dynamic-extended   Extend the dynamic ACL absolute timer
  rate-limit         Simple rate-limit specific access list

SW1(config)#do sh access-list
Extended IP access list manage
    10 permit tcp host 192.168.60.0 0.0.0.253 192.168.3.2
    20 permit tcp host 192.168.60.0 0.0.0.253 192.168.3.2 eq telnet
    30 permit ip any any
Extended IP access list sl_def_acl
    10 deny tcp any any eq telnet
    20 deny tcp any any eq www
    30 deny tcp any any eq 22
    40 permit ip any any
SW1(config)#
```

Fig 12. Restrict Management Access

D. *Enable Network Time Protocol (NTP)*

This step is essential for enable logging, which is useful for monitoring, incident response and auditing, the system have accurate and uniform clock settings on all network devices in order for log data to stamp with the correct time and time zone.

This will help extremely incident handling and proper log monitoring and correlation as shown in Fig 13.



```
SW1#sh ntp s
SW1#sh ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz, precision is 2**17
reference time is 00000000.00000000 (21:01:00.000 UTC Thu Dec 31 1899)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
SW1#sh cl
SW1#sh cl
SW1#sh cl
SW1#sh clo
SW1#sh clock
.10:11:20.498 UTC Mon Jul 5 2021
SW1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#cl
SW1(config)#clo
SW1(config)#clock t
SW1(config)#clock timezone PST +2
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
01:10:13: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:12:33 UTC Mo
n Jul 5 2021 to 15:11:33 PST Mon Jul 5 2021, configured from console by console.
SW1(config)#DO WR
Building configuration...
[OK]
```

Fig 13. NTP Status

E. *Enabling Port Fast and BPDU Guard on a Port*

Bridge protocol data unit (BPDU) guard feature is one of the spanning tree protocol (STP) enhancements. This feature enhances switch network reliability, manageability, and security.

When a STP BPDU is received on a BPDU guard enabled port, the port is shut down and the state of the port changes to error-disable (ErrDis) state. The port remains in the ErrDis state until the port status is manually changed by using the configuration command shut followed by a no-shut applied on the interface.

VIII. Kali Linux Penetration Test

Kali Linux tools are used to test the network security system after enabling security policy's features in the AD and core switches (IP Kali Linux (192.168.2.201)) as described in Fig 14.

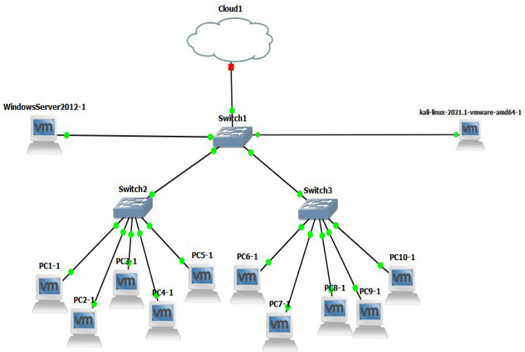
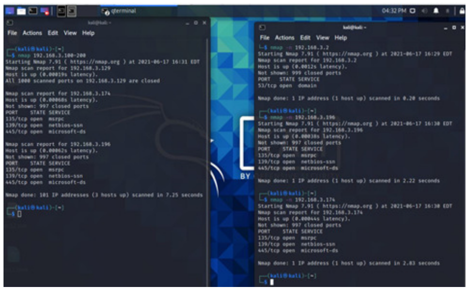


Fig 14. Connect Kali Linux to the Network System.

A. Nmap

After enabling security policy's features in the AD and core switches, it observed that whole ports are closed except the indispensable ports as described in Fig 15.



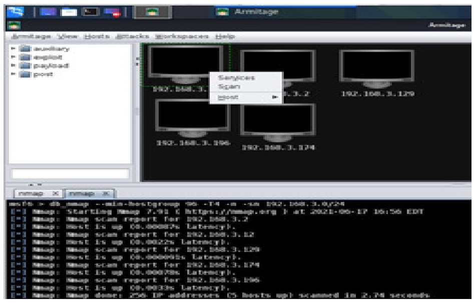
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.3.100-200
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 16:31 EDT
Nmap scan report for 192.168.3.129
Host is up (0.00019s latency).
All 1000 scanned ports on 192.168.3.129 are closed

Nmap scan report for 192.168.3.174
Host is up (0.00068s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap scan report for 192.168.3.196
Host is up (0.00062s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 101 IP addresses (3 hosts up) scanned in 7.25 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

```
└─$ nmap -n 192.168.3.2
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 16:29 EDT
Nmap scan report for 192.168.3.2
Host is up (0.0012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -n 192.168.3.196
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 16:30 EDT
Nmap scan report for 192.168.3.196
Host is up (0.00038s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 2.22 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -n 192.168.3.174
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 16:30 EDT
Nmap scan report for 192.168.3.174
Host is up (0.00044s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Fig 15. Nmap

B. Armitage

Data execution prevention (DEP) is a system-level memory protection feature available in windows OS. DEP enables the OS to mark one or more pages of memory as non-executable, which prevents code from being run from that region of memory, to help prevent exploitation of buffer overruns.



```
msf6 > db_nmap --min-hostgroup 96 -T4 -n -sn 192.168.3.0/24
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-17 16:56 EDT
[*] Nmap: Nmap scan report for 192.168.3.2
[*] Nmap: Host is up (0.00087s latency).
[*] Nmap: Nmap scan report for 192.168.3.12
[*] Nmap: Host is up (0.0022s latency).
[*] Nmap: Nmap scan report for 192.168.3.129
[*] Nmap: Host is up (0.000095s latency).
[*] Nmap: Nmap scan report for 192.168.3.174
[*] Nmap: Host is up (0.00070s latency).
[*] Nmap: Nmap scan report for 192.168.3.196
[*] Nmap: Host is up (0.0033s latency).
[*] Nmap: Nmap done: 256 IP addresses (5 hosts up) scanned in 2.74 seconds
```

Fig 16. Not Finding a Suitable Attack

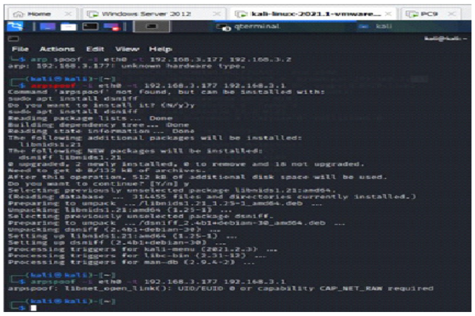
DEP helps prevent code from being run from data pages such as the default heap, stacks, and memory pools. Although some applications have compatibility problems with DEP, the vast majority of applications do not.

Enable (DEP) feature prevents programs from running in the background, protecting the device from attacks as described in Fig 16.

C. Arpspoof

BPDU Filter feature also can be enabled on an access port that should never receive a BPDU. If a switch port which is configured with STP port fast feature, it must be connected to an end device.

The STP port fast is enabled only on access ports to speed up the transition of access port to STP forwarding state. End devices are not supposed to generate BPDUs, because in a normal network environment, BPDU messages are exchanged by network switches as respectively described in Fig 17.

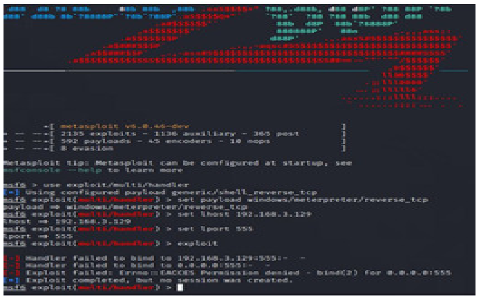


```
└─$ arp spoof -i eth0 -t 192.168.3.177 192.168.3.2
arp: 192.168.3.177: unknown hardware type.

┌──(kali㉿kali)-[~]
└─$ arpspoof -i eth0 -t 192.168.3.177 192.168.3.1
Command 'arpspoof' not found, but can be installed with:
sudo apt install dsniff
Do you want to install it? (N/y)y
sudo apt install dsniff
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  libnids1.21
The following NEW packages will be installed:
  dsniff libnids1.21
0 upgraded, 2 newly installed, 0 to remove and 18 not upgraded.
Need to get 0 B/132 kB of archives.
After this operation, 512 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Selecting previously unselected package libnids1.21:amd64.
(Reading database ... 314455 files and directories currently installed.)
Preparing to unpack .../libnids1.21_1.25-1_amd64.deb ...
Unpacking libnids1.21:amd64 (1.25-1) ...
Selecting previously unselected package dsniff.
Preparing to unpack .../dsniff_2.4b1+debian-30_amd64.deb ...
Unpacking dsniff (2.4b1+debian-30) ...
Setting up libnids1.21:amd64 (1.25-1) ...
Setting up dsniff (2.4b1+debian-30) ...
Processing triggers for kali-menu (2021.2.3) ...
Processing triggers for libc-bin (2.31-12) ...
Processing triggers for man-db (2.9.4-2) ...

┌──(kali㉿kali)-[~]
└─$ arpspoof -i eth0 -t 192.168.3.177 192.168.3.1
arpspoof: libnet_open_link(): UID/EUID 0 or capability CAP_NET_RAW required

┌──(kali㉿kali)-[~]
└─$ 
```

Fig 17. Tricked of the Victim's Device as a Router

D. Metasploit Framework

The Metasploit framework consists of exploits, payloads, modules, plugin’s and scripts. The main concept is that run exploits and payloads in the background. Enable (DEP) feature prevents programs from running in the background as described in Fig 18.



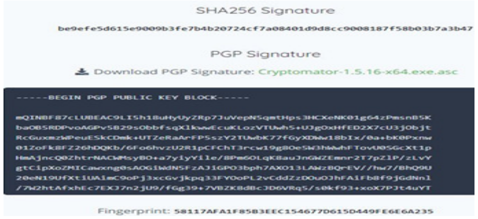
```
       =[ metasploit v6.0.46-dev                          ]
+ -- --=[ 2135 exploits - 1138 auxiliary - 365 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.3.129
lhost => 192.168.3.129
msf6 exploit(multi/handler) > set lport 555
lport => 555
msf6 exploit(multi/handler) > exploit

[-] Handler failed to bind to 192.168.3.129:555:-  -
[-] Handler failed to bind to 0.0.0.0:555:-  -
[-] Exploit failed: Errno::EACCES Permission denied - bind(2) for 0.0.0.0:555
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > 
```

Fig 18. DEP Stopped App Execute/Untrusted Exploit

E. Mechanism of Encrypting and Storing Data in Cloud

Using the cryptomator server through the keys algorithms makes data securely protected against ransomware, viruses, data theft, unauthorized access and data loss. The advantage of the cryptomator server are:

1. User management which is compatible with AD/ lightweight directory access protocol (LDAP)
2. Malware protection
3. Self-learning ransomware detection by measurement of entropy change.
4. Automatic virus scan
5. Audit logs which is traceability of file accesses
6. Automatic account blocking in case of suspicious activities
7. Encryption which is AES-GCM (256 bit) encryption of files before storage and cloud synchronization
8. Based on award-winning and 1&1-audited Cryptomator technology
9. Cloud backup
10. Automatic synchronization of encrypted files
11. Easy recovery of files and file versions



SHA256 Signature

be9efe5d615e9009b3fe7b4b20724cf7a08401d9d8cc9008187f58b03b7a3b47

PGP Signature

Download PGP Signature: Cryptomator-1.5.16-x64.exe.asc

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBF87cLUBEAC9LISh18uHyUyZRp7JuVepN5qmtHps3HCXeNK01g64zPmsnB5K
baOB5RDPvoAGPv5829sObbfsqXlkwwEcuKLozVTUwh5+UJg0xHfED2X7cU3jObjt
RcGuxmzWPeuESkCDmk+UTZeRaArFP5szY2TUwbK77fGyXDWw18bIx/0a+bK0Pxnw
01ZoFk8FZ26hDQKb/6Fo6hvzU2R1pCFChT3rcw19g8Oe5W3hWwhFTovU05GcXt1p
HmAjncQ0ZhtrNACWMsyBO+a7yiyYile/8Pm6OLqK8auJnGWZEmnr2T7pZlP/zLvY
gtCipXoZMICawxng0sAOGiWdN5FzAJ1GPO3bph7AXO13LAWzBQrEV//hw7/BhQ9U
20eN19UfXtiUAimC9oPj3xcGvjkpq33FYOoPL2vCddZzDOuOJhFA1Fb8f9jGdNnl
/7W2htAfxhEc7EXJ7n2jU9/fGg39+7VBZK8dBcJD6VRq5/s0kf93+xoX7PJt4uYT
```

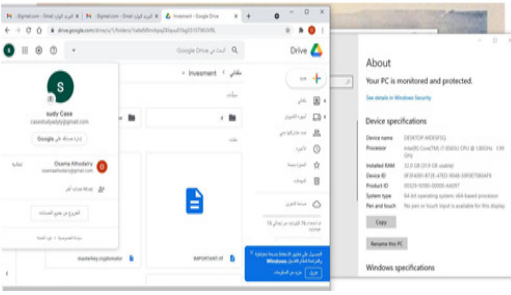
Fingerprint: 58117AFA1F85B3EEC154677D615D449FE6E6A235

Fig 19. Key SHA256

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQINBF87cLUBEAC9LISh18uHyUyZRp7JuVepN5qmtHps3HCXeNK01g64zPmsnB5K
baOB5RDPvoAGPv5829sObbfsqXlkwwEcuKLozVTUwh5+UJg0xHfED2X7cU3jObjt
RcGuxmzWPeuESkCDmk+UTZeRaArFP5szY2TUwbK77fGyXDWw18bIx/0a+bK0Pxnw
01ZoFk8FZ26hDQKb/6Fo6hvzU2R1pCFChT3rcw19g8Oe5W3hWwhFTovU05GcXt1p
HmAjncQ0ZhtrNACWMsyBO+a7yiyYile/8Pm6OLqK8auJnGWZEmnr2T7pZlP/zLvY
gtCipXoZMICawxng0sAOGiWdN5FzAJ1GPO3bph7AXO13LAWzBQrEV//hw7/BhQ9U
20eN19UfXtiUAimC9oPj3xcGvjkpq33FYOoPL2vCddZzDOuOJhFA1Fb8f9jGdNnl
/7W2htAfxhEc7EXJ7n2jU9/fGg39+7VBZK8dBcJD6VRq5/s0kf93+xoX7PJt4uYT
[illegible]
=/rFy
-----END PGP PUBLIC KEY BLOCK-----
```

Fig 20. Key ASE

Performance the encrypting and hiding the files, then store them in the cloud, till the last step, which is showing the files in google drive as encrypted and how it appears to another google drive user as described respectively trough Fig 19, Fig 20 and finally, data in google drive was encrypted as described in Fig 21.



About

Your PC is monitored and protected.

See details in Windows Security

Device specifications

Copy

Rename this PC

Windows specifications

Fig 21. Files in Google Drive as Encrypted

IX. Conclusions

This study presents an effective framework for protecting SMEs from cybersecurity risks and threats in the cloud environment. Case study and evaluations, like the one mentioned, provide valuable insights into the effectiveness of cloud security policies and frameworks. By conducting penetration testing and performance assessments, organizations can identify vulnerabilities, address potential weaknesses, and continuously improve their cloud security measures.

By leveraging encryption, VPN tunnels, and penetration testing, organizations can enhance their security measures and safeguard their sensitive data. Implementing such a framework can help SMEs maintain regulatory compliance, protect customer privacy, and ensure the confidentiality and integrity of their data in the cloud.

References

[1] Timothy Langan "Internet Crime Report", Federal Bureau of Investigation,https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf , 2022.

[2] Financial Crimes Enforcement Network "The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic", *press release*, 3 April 2020.

[3] Financial Industry Regulatory Authority "Cybersecurity Alert: Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19)", *Information Notice*, 26 March 2020.

[4] Cyber Crime Wing, "Cyber Crimes Risks, Prevention and Legal Remedies", Guidelines for Cyber Users, *Federal Investigation Agency, Ministry of Interior, Government of Pakistan*, 2022.

[5] James Babbage "Ransomware, extortion and the cybercrime ecosystem", A white paper from the *National Cyber Security Center (NCSC) and the National Crime Agency (NCA)*, 2022.

[6] Usman Tariq, Irfan Ahmed, Ali Kashif and Kamran Shaukat "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review", *Sensors,* 23(8), 4117, https://doi.org/10.3390/s23084117, 2023/

[7] Kristina Rigopoulos, "Updating the NIST Cybersecurity Framework", NIST, Journey To CSF 2.0, https://www.nist.gov/, 2023.

[8] US Securities and Exchange Commission (SEC), "Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure", USA, https://www.sec.gov/rules/proposed/2022/33-11038.pdf, February 2022.

[9] US Committee of Sponsoring Organizations of the Treadway Commission (COSO), "Guidance on Enterprise Risk Management (ERM)", https://www.coso.org/SitePages/Guidance-on-Enterprise-Risk-Management.aspx?web=1, April 2022.

[10] Cao, C.; Tang, Y.; Huang, D.; Gan, W.; Zhang, C. IIBE "An Improved Identity-Based Encryption Algorithm for WSN Security", Secur.Commun.Netw, 1–8, 2021.

[11] NIST "Cybersecurity Framework. Cybersecurity", Version 1.1. 12. Available: https://www.nist.gov/cyberframework, 5 January 2022.

[12] Wani, A.R.; Gupta, S.K.; Khanam, Z.; Rashid, M.; Alshamrani, S.S.; Baz, M. "A novel approach for securing data against adversary attacks in UAV embedded HetNet using identity based authentication scheme", *IET Intell*. Transp. Syst. Early View, 1–19, 2022.

[13] Jon Welling "What Is the Cloud Secure Data Lifecycle", CBT Nuggets, https://www.cbtnuggets.com/blog/certifications/cloud/what-is-the-cloud-secure-data-lifecycle, July 2022.

[14] IBM and Cisco "An overview of cloud security", https://www.ibm.com/topics/cloud-security, 2023.

[15] Sheikhpour, S.; Ko, S.B.; Mahani, A. "A low cost fault-attack resilient AES for IoT applications", Microelectron. Reliab, 123, 114202, 2021.

[16] Sreekanth, M.; Jeyachitra, R. "Implementation of area-efficient AES using FPGA for IOT applications", Int. J. Embed. Syst, 15, 354, 2022.

[17] Orion Cassetto "Cybersecurity Threats: Everything you Need to Know", exabeam, https://www.exabeam.com/information-security/cyber-security-threat/, February 01, 2023.

[18] Frank. C, Barry. S, Michael. F, Arash. Kia, Martin. M, Finbarr. M and Stefan. M "Cyber risk and cybersecurity: a systematic review of data availability", https://link.springer.com/article/10.1057/s41288-022-00266-6, volume 47, 698–736, 7, 2022.

[19] amir, M., S.S.H. Rizvi, M.A. Hashmani, M. Zubair, and J. Ahmad "Machine learning classification of port scanning and DDoS attacks A comparative analysis", Mehran University Research Journal of Engineering and Technology 40 (1): 215–229, 2021.

[20] Aassal, A. El, S. Baki, A. Das, and R.M. Verma "An in-depth benchmarking and evaluation of phishing detection" research for security needs. *IEEE Access* 8: 22170–22192, 2020.

[21] Yuchong Li and Qinghui Liu "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments", Energy Reports, *Elsevier*, Volume 7, November, 8176-8186, 2021.