

Research Report Cybersecurity

by Valentin Blazhev

Submission date: 20-Jul-2023 05:51PM (UTC+0100)

Submission ID: 210475047

File name: 30086_Valentin_Blazhev_Research_Report_Cybersecurity_507624_1858094173.docx (890.15K)

Word count: 6095

Character count: 35494

Programme: BSc (Hons) Cloud Computing

Module: Advanced Cyber Security

(ACCB6000_BIRM)

|StudentID:2026380|

A Research Report for LENDING HANDS to Resolve Cybersecurity Threats

23

Contents

I. Abstract:	1
II. Introduction:	2
III. Literature Review:	3
IV. Research Methodology:	4
V. Proposed Methods to Resolve Cybersecurity Threats:	6
VI. Implementation and Analysis:	7
VII. Conclusive Note:	18
VIII. REFERENCES	19

I. Abstract:

This research paper addresses the cybersecurity risks faced by the non-profit organization "Lending Hands" and offers workable remedies. An extensive summary of the most recent advancements and research in the topic of cybersecurity is given at the beginning of the article. It covers a wide range of topics, such as current threats, vulnerabilities, and defense strategies. Based on the findings of the investigation, the paper describes the primary cybersecurity threats to which the NGO is vulnerable. These hazards include network security, vulnerability assessment, and personnel knowledge and training. Increasing staff knowledge and training, boosting network security, and performing regular vulnerability assessments are among the suggested solutions to address these risks. Additionally, the paper has a part on implementation and analysis where several tools are utilized for scanning, enumeration, vulnerability analysis, and ethical hacking tasks. Finally, a thorough mitigation approach is suggested, taking into account the NGO's tangible and intangible assets. The strategy offers specific suggestions to reinforce the NGO's cyberspace and tries to assist the organization in understanding its technological security flaws.

II. Introduction:

In recent years, organizations from all industries, including non-governmental organizations (NGOs), have made cybersecurity a major concern due to the growing reliance on digital technology and the interconnectedness of cyberspace. The use of digital technologies in routine operations exposes businesses to a variety of cybersecurity risks, as the "Lending Hands" NGO example demonstrates. It is essential to perform in-depth study and analysis of existing trends, new threats, vulnerabilities, and defense mechanisms in the cybersecurity environment in order to successfully handle these challenges.

Research shows that cyber assaults have become more frequent and more sophisticated over time. Phishing was the most often recognized attack vector, according to the Cyber Security Breaches Survey 2022 (Department for Digital, Culture, Media & Sport, 2022), which found that 39% of organizations had experienced a cyber assault. According to Singh and Nene (2013), this emphasizes the urgent need for organizations, especially NGOs, to upgrade their cybersecurity procedures and create effective risk-mitigation plans.

An extensive examination of current research and industry breakthroughs is necessary to suggest viable solutions to the cybersecurity concerns faced by the "Lending Hands" NGO. This study need to include a wide variety of subjects, such as current threats and vulnerabilities, new attack vectors, defensive strategies, and suggested risk-mitigation measures.

Understanding the diverse variety of research being conducted in the sector requires a thorough assessment of the literature. It assists in locating pertinent research and viewpoints that support the suggested approaches. For example, studies by Van Haastrecht et al. (2021) and Habibzadeh et al. (2019) offer important insights into the present-day threats, weaknesses, and defense strategies in the cybersecurity environment. These studies emphasize the value of proactive defensive strategies, the dissemination of threat intelligence, and staff training as means of reducing cybersecurity risks.

Additionally, recent studies investigating the potential of machine learning and artificial intelligence in boosting cybersecurity measures include those by Mazhar et al. (2023) and Singh and Nene (2013). By offering sophisticated intrusion detection systems, anomaly detection algorithms, and predictive analytics to recognize and address new risks, these developments can considerably improve the offered techniques.

Recent cybersecurity breaches and their ramifications are also examined in the study for this paper. Analysis of case studies and publications, such the Verizon Data Breach Investigations Report (Verizon, 2023), can provide insights into the attack strategies used by threat actors and the most frequently exploited vulnerabilities. This information is essential for developing mitigation techniques that effectively address certain vulnerabilities and possible points of attack.

The study also takes into account the value of staff education and awareness in enhancing cybersecurity defenses. Studies by Khando et al. (2021) and Habibzadeh et

al. (2019) highlight the need of ongoing training programs, simulating phishing attacks, and educating staff members on social engineering tactics. These results will emphasize the need to prioritize staff training and create a security-aware culture inside the firm and will inform the suggested strategies for the "Lending Hands" NGO.

In conclusion, the digital revolution has elevated cybersecurity to a critical position within business operations. Conducting in-depth research and analysis is essential to address the cybersecurity concerns faced by NGOs like "Lending Hands." Recent dangers, weaknesses, defensive strategies, and upcoming technologies may all be learned a lot about by reading current literature, research papers, and industry reports. The suggested approaches should make use of this information to create thorough plans that reduce risks, fortify defenses, and encourage an atmosphere inside the firm that is concerned with cybersecurity.

III. Literature Review:

Organizations must keep up with the most recent developments in attack methods and defense strategies because cybersecurity threats are always changing. With an emphasis on phishing attacks, network security concerns, and best practices for reducing these risks, this literature review intends to evaluate new research and studies in relation to cyber threats and defense mechanisms. Additionally, the value of staff education and awareness in strengthening cybersecurity posture will be emphasized.

One of the most popular and successful ways for thieves to acquire sensitive data without authorization is through phishing assaults. Phishing attacks use human psychology and social engineering approaches to trick people into exposing their private information, according to research by Dhamija, Tygar, and Hearst (2006). Numerous research have suggested various defensive strategies to counter this hazard.

The use of authentication protocols is one such technique. Implementing robust authentication techniques, such as two-factor authentication (2FA) or biometric authentication, can dramatically lower the likelihood of falling victim to phishing attempts, according to research by Tembe (2014). By requesting a second form of identification from users, these measures create an extra layer of protection and make it harder for attackers to acquire illegal access.

Addressing network security concerns is a crucial component of cybersecurity. Securing networks has become a vital problem because to the proliferation of Internet of Things (IoT) devices and the growing interconnection of gadgets. Research by Khan et al. (2022) underlines the necessity for strong network security measures and identifies possible vulnerabilities posed by IoT devices.

Implementing intrusion detection systems (IDS) is one method for reducing network security concerns. These programs keep an eye on network traffic for any unusual activity or attempts at illegal access. IDS can successfully identify and react to a variety of threats, including network-based attacks like distributed denial-of-service (DDoS) attacks and malware infections, according to study by Lazarevic et al. (2003).

Network segmentation has also been recognized as a useful tactic for boosting network security. According to Mhaskar Alabbad and Khedri's (2021) research, segmenting networks into smaller, more isolated groups may help prevent lateral attacker movement in the case of a breach. This strategy lessens the potential effect of a cyber assault by making it difficult for attackers to access sensitive information and vital systems.

Employee education and awareness are vital in the context of cybersecurity for preventing security breaches. The necessity of training staff members about cybersecurity threats and effective practices is emphasized by Willie's research (2023). Employees are frequently the weakest link in an organization's security chain because they might unwittingly fall prey to social engineering assaults or participate in dangerous actions, as this article emphasizes.

It is advised that employers provide ongoing staff training programmes to mitigate this issue. Studies by Alrobaian Alshahrani, and Almaleh (2023), as well as Hijji and Alam (2022), indicate the value of simulated phishing training for increasing employee understanding of attacker techniques. These training sessions imitate actual phishing attacks and teach employees how to spot and report questionable emails and texts.

A security-conscious culture must be established within an organisation, too. According to Da Veiga's (2016) research, companies should encourage their staff to feel accountable for cybersecurity. This may be accomplished by establishing channels for staff to report security issues or request assistance, as well as by communicating often and reminding them of security regulations.

Consequently, the literature study has investigated current developments in cyber threats and defence mechanisms, concentrating on phishing assaults, network security hazards, and the significance of staff knowledge and training. The study emphasises the need of putting robust authentication mechanisms in place to prevent phishing attempts, such two-factor authentication and biometric authentication. It also emphasises the necessity of strong network security measures, such as network segmentation and intrusion detection systems. The analysis also highlights how crucial it is to have ongoing employee training programmes and a security-conscious organisational culture. Organisations may improve their cybersecurity posture and lower their risk of falling victim to online attacks by using these recommended practises.

IV. Research Methodology:

An extensive examination of scholarly works, business reports, and case studies was done in order to perform this research. Emerging dangers, technical developments, and suggested defensive strategies were among the main research topics. The results were examined in order to offer practical solutions to the NGO's cybersecurity challenges.

Cybersecurity Risks Analysis:

The NGO confronts many cybersecurity concerns in the scenario given. These include the possibility for network vulnerabilities, phishing attempts, and unauthorised access to private data. Additional hazards are introduced by the shared facility agreement with other enterprises. The research points out the significant areas of concern listed below:

Awareness and Training of Employee:

Many employees have not finished the required cybersecurity training or studied the recommended practises despite email reminders and the implementation of the policy. This ignorance makes people more susceptible to phishing scams and other social engineering tricks.

The absence of personnel education and awareness puts the NGO's cybersecurity at serious danger. Studies have emphasised the value of staff knowledge and training as a key line of defence against cyber dangers. Employee training programmes considerably minimise the vulnerability to phishing attempts, according to study by Alkhalil et al. (2021). According to the report, businesses with thorough training programmes saw fewer successful phishing attempts. This emphasises the necessity for ongoing and successful training programmes to reduce cybersecurity threats.

A study by Khan et al. (2022) also emphasises the link between staff knowledge and cybersecurity issues. According to the report, companies with poor employee cybersecurity knowledge are more vulnerable to data breaches and unauthorised access. This emphasises how important training is in lowering the possibility of successful cyberattacks.

Security of Network:

Network security risks may exist since the NGO shares the space with other enterprises. The likelihood of unauthorised access, data breaches, and malware outbreaks rises when there are several organisations present.

The need of network security measures to guard against unauthorised access and data breaches is emphasised by research studies. Liang et al. (2020) talk about the importance of network segmentation as a defence mechanism in their study. Network segmentation can be put into place to separate crucial systems and limit unauthorised access. Network segmentation improves security, according to the study report, by keeping possible attacks inside designated segments and reducing their influence on the overall network.

Additionally, a Roy et al. (2020) research emphasises the value of proactive methods, such as vulnerability management, in preserving network security. To lower the risk of network intrusions, regular vulnerability assessment and prompt repair of found holes are essential. To successfully detect, prioritise, and remedy vulnerabilities, the research report emphasises the necessity for a thorough vulnerability management methodology.

Assessment of Vulnerability :

It's essential to conduct regular vulnerability scanning to find and fix flaws in the network architecture. Without a thorough review, possible weaknesses can go undiscovered, leaving the NGO more open to assaults.

The importance of vulnerability assessment in maintaining a strong cybersecurity posture is highlighted in research articles. The advantages of vulnerability scanning tools in locating and addressing network vulnerabilities are covered in a research by Saxena et al. (2020). In order to effectively analyse vulnerabilities, the research report recommends utilising tools like OpenVAS or Nexpose and emphasises the importance of ongoing scanning to find new vulnerabilities.

36

A study by Shah et al. (2021) also highlights the value of penetration testing in locating network problems. Penetration testing, commonly referred to as ethical hacking, aids in simulating actual attack scenarios to pinpoint weaknesses and evaluate the efficacy of current security measures. The study report emphasises penetration testing's critical role in vulnerability assessment as a means of proactively identifying and addressing possible flaws.

Since staff awareness and training, network security, and vulnerability assessment are the key areas of concern, they are highlighted in the study of the cybersecurity threats faced by the "Lending Hands" NGO. The citations to the research publications mentioned above serve as proof of the significance of these topics in reducing cybersecurity threats. The NGO may improve its cybersecurity posture and fend off attacks by putting in place efficient training programmes, network security measures, and frequent vulnerability assessments.

V. Proposed Methods to Resolve Cybersecurity Threats:

The following techniques are suggested to reduce the identified cybersecurity threats and strengthen the NGO's security posture in light of the research carried out:

Strengthen Employee Awareness and Training:

- a. Hold routine cybersecurity training sessions to inform staff about typical risks and recommended procedures (Hijji and Alam, 2021).
- b. Put in place a tracking mechanism to verify that all required training modules have been completed and to evaluate the success of training initiatives (Chowdhury and Gkioulos, 2023).
- c. Create a strategy for internal communication to enforce cybersecurity guidelines and deliver regular updates and reminders (Charlet, 2018).

Enhance Network Security:

- a. Use network segmentation to keep vital systems apart from other companies using the same space as them (Mhaska, Alabbad, and Khedri, 2021).
 - b. All network devices and systems should be patched and updated on a regular basis to fix known vulnerabilities (Kejiou and Bekaroo, 2022).
- Utilise intrusion detection and prevention systems (IDPS) to keep an eye on network activity and spot possible attacks (Azeez et al., 2020).

d. Use MFA (multi-factor authentication) for network resources that can be accessed remotely (Das et al., 2019).

Conduct Regular Vulnerability Assessments:

To find network vulnerabilities, use alternate vulnerability scanning tools as OpenVAS or Nexpose (Aslan et al., 2023).

b. Carry out routine penetration testing to evaluate the efficacy of current security measures and spot any possible vulnerabilities (Vats, Mandot, and Gosain, 2020).

c. Create a vulnerability management procedure to sort and address vulnerabilities that have been found (Aslan et al., 2023).

VI. Implementation and Analysis

The implementation and analysis of different scanning, enumeration, vulnerability assessment, and ethical hacking activities will be the main topics of this part. The goal is to utilise alternative tools, record the workflow, take screenshots, and evaluate the outcomes. Let's explore each action in further depth.

Activity 1: Scanning and Enumeration

Part 1: HPING ¹⁴ alternate to send ICMP/TCP/UDP Packets and analyze the target replies.

Part 2: MegaPing ¹⁴ alternative tool to identify live hosts and open ports of the Target.

Part 3: NetScanTools Pro ¹⁴ alternate to initiate various Scans.

Implementation:

We will utilise the alternative tool Nmap, a flexible network scanning tool, to complete this assignment. We may send ICMP, TCP, and UDP packets to a target and then use Nmap to examine the answers. Conduct TCP Connect Scan and SYN Scan on the target system to find live hosts and open ports. The actions listed below were taken:

- Install Nmap on your computer.
- Run the following command in the terminal: `nmap -sP "target IP"`
- Nmap asks for and gets ICMP echo responses from the target IP. Additionally, it offers details on the active hosts connected to the network.

```
File Actions Edit View Help
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
```

Analysis:

We were able to send ICMP packets to the target IP and get ICMP responses by using Nmap. This aids in locating the network's active hosts. The data gathered from this activity may be utilised to comprehend network structure and pinpoint possible targets for more investigation and evaluation. In addition, we were able to locate the active hosts inside the target IP range and find the open ports on those hosts. Understanding the network architecture and spotting any weaknesses linked to the exposed ports are made easier with the use of this information. Last but not least, we may use a variety of scans, such TCP Connect Scan and SYN Scan, to find open ports, services that are using them, and any potential security flaws connected to them.

Part 4: Investigate various network scanning methods.

Implementation:

We will use the alternative tool nmap, a potent vulnerability scanning tool, to investigate several network scanning methods. Nmap offers a variety of scanning tools and methods to find weaknesses in the target network. The subsequent actions were taken:

- Launch nmap and select the target IP address or range as well as other scan parameters.

- Select the appropriate scan template, such as a web application scan or a comprehensive scan.
- Start the scan, then watch for the output of the findings.

```

root@kali: ~
File Actions Edit View Help
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
(root@kali)~# nmap -sO
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-18 03:49 BST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.01 seconds
(root@kali)~#

```

Analysis:

We were able to investigate several network scanning strategies using nmap to find vulnerabilities in the target network. We can find possible flaws that hostile actors may use by using the tool's thorough scanning capabilities and huge vulnerability database.

Part 5: Using a substitute for Proxy Switcher to remain anonymous online.

Implementation:

We will use the free alternative programme Tor Browser to be anonymous online. Through the use of a network of relays, the free and open-source programme Tor enables anonymous communication over the internet. These are the steps involved:

- Install Tor Browser on the computer by downloading it.
- Open the Tor browser and connect to the Tor network.
- Set your browser to block tracking cookies and disable JavaScript to guarantee your anonymity.
- Use the Tor Browser to access the internet.

Analysis:

For maintaining online anonymity, Tor Browser is a good substitute for Proxy Switcher. Our internet data is routed via numerous nodes using Tor's relay network, making it challenging to identify the communication's source and destination. This improves online surfing security and privacy.

Part 6: TTL to identify Target Operating System.

Implementation:

Using the alternative tool Xprobe2, we can determine the target operating system by looking at the TTL (Time To Live) number. An active OS fingerprinting tool called Xprobe2 delivers bogus packets to a target machine and examines the response's TTL value. The following are the stages for implementation:

- Install Xprobe2 on the computer.
- Launch a terminal and enter the following command: Target IP: xprobe2 -T4
- In order to identify the OS system, Xprobe2 sends forged packets to the target IP and examines the TTL value in the answers.

Analysis:

By examining the TTL values in the answers, we were able to determine the target OS system by using Xprobe2. This method helps identify possible vulnerabilities unique to the detected operating system and offers useful information about the target system's underlying architecture.

Part 7: An automatic tool to Map a Network.

Implementation:

We will use the alternative tool OpenNMS, an open-source network management platform, to automatically map the network. Maltego provides functionality for network discovery and mapping that provide users a thorough understanding of the network infrastructure. The following actions are taken:

- Set up OpenNMS on the computer.
- OpenNMS should be launched, and network discovery parameters should be established.
- Start the network discovery procedure so that the network may be automatically mapped.
- To learn more about the topology of the network, analyse the created network map.

Analysis:

We automated network mapping using OpenNMS, enabling us to see the network infrastructure and recognise associated devices. We can grasp the links between devices and spot possible weak spots by using the network map, which gives a visual depiction of the network topology.

Part 8: Enumerate using NetBIOS.

Implementation:

We will use the other utility enum4linux to carry out NetBIOS enumeration. Enum4linux is a command-line programme that looks up NetBIOS data from networked devices. These are the stages involved in this activity:

- enum4linux retrieves device names and MAC addresses from the devices in the specified IP range after querying their NetBIOS information.

```
-# enum4linux -n 10.10.0.50
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux )

-----
| Target Information |
-----
Target ..... 10.10.0.50
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

-----
| Enumerating Workgroup/Domain on 10.10.0.50 |
-----
[*] Got domain/workgroup name: WORKGROUP

-----
| Netstat Information for 10.10.0.50 |
-----
Looking up status of 10.10.0.50
NETASPLISTABLE <00> - 8 <ACTIVE> Workstation Service
NETASPLISTABLE <03> - 8 <ACTIVE> Messenger Service
NETASPLISTABLE <20> - 8 <ACTIVE> File Server Service
...MSBROWSE <01> - <GROUP> 8 <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> 8 <ACTIVE> Domain/Workgroup Name
WORKGROUP <1b> - 8 <ACTIVE> Master Browser
WORKGROUP <1a> - <GROUP> 8 <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

-----
| Session Check on 10.10.0.50 |
-----
[*] Server 10.10.0.50 allows sessions using username '', password ''

-----
| Getting domain SID for 10.10.0.50 |
-----
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[*] Can't determine if host is part of domain or part of a workgroup
enum4linux complete on Wed May 22 15:45:41 2019
```

Analysis:

We were able to enumerate NetBIOS data from the target devices inside the given IP range by using enum4linux. With the use of this data, devices may be recognised by their names and MAC addresses, which can then be used for further investigation and potential exploitation.

Part 9: Nmap and enum4linux to Enumerate.

Implementation:

We will combine the features of enum4linux and Nmap to carry out enumeration. The live hosts and open ports will be found using Nmap, and the shares and resources on the found hosts will be found using Net Use. These are the steps involved:

- Use Nmap to find active hosts and open ports, as was previously indicated.
- Use the enum4linux command to list shares and resources on the target hosts once the live hosts and open ports have been located.

Analysis:

We were able to effectively enumerate the target hosts by combining the features of Nmap and enum4linux. Nmap helped us locate active hosts and open ports, and the enum4linux command informed us of the shares and resources that were accessible on

those hosts. This enumeration procedure assists in compiling data on the file-sharing infrastructure of the network and potential points of unauthorised access.

Activity 2: Vulnerability Assessment

We will use a variety of technologies in this activity to do network vulnerability analysis and vulnerability scanning.

Task 1: Nessus tool alternate in Windows to scan for network vulnerabilities.

Implementation:

We will use the open-source vulnerability detection alternative programme OpenVAS for this purpose. A full range of vulnerability testing and reporting on found vulnerabilities are offered by OpenVAS. These are the steps involved:

- Put OpenVAS on the Windows machine.
- Launch the OpenVAS programme and select the scan parameters, including the target IP address or range.
- Start the scan, then watch for the output of the findings.
- Analyse the vulnerability report that was created to find and rank vulnerabilities.

Analysis:

We carried out vulnerability scanning on the target network, particularly on a Windows PC, using OpenVAS. The programme effectively located the network's vulnerabilities, providing thorough details and severity rankings for each one. This makes it easier to prioritise corrective actions to reduce possible dangers.

Task 2: Nessus tool alternative in Kali Linux to scan for network vulnerabilities.

Implementation:

We will use Nexpose, an alternate tool for vulnerability management and assessment, for this work. Nexpose creates thorough reports and offers a variety of vulnerability detection tools. The following are the stages for implementation:

- Install Nexpose on the Kali Linux system, then launch it and set the scan parameters, such as the target IP address or range.
- Start the scan, then watch for the results to appear.
- Analyse the vulnerability report that was created to find and rank vulnerabilities.

The screenshot shows the Nexpose web interface. At the top, there are tabs for Assets, Vulnerabilities, Policies, Reports, and Administration. Below these, there's a 'Scan Progress' section with a table showing a completed manual scan on 10/7/2014. The 'Discovered Assets' section shows a table with two assets: 192.168.1.1 (Microsoft Windows 7 Ultimate Edition SP1) and 192.168.1.2 (Microsoft Windows 7 Ultimate Edition SP1).

Scan Type	Started	Assets	Vulnerabilities	Elapsed	Status
Manual	10/7/2014 10:26:47 AM	2	11	2 minutes	Completed successfully

Address	Name	Operating System	Vulnerabilities	Scan Duration	Scan Status
192.168.1.1		Microsoft Windows 7 Ultimate Edition SP1	11	2 minutes	Completed
192.168.1.2		Microsoft Windows 7 Ultimate Edition SP1	0	26 seconds	Completed

Analysis:

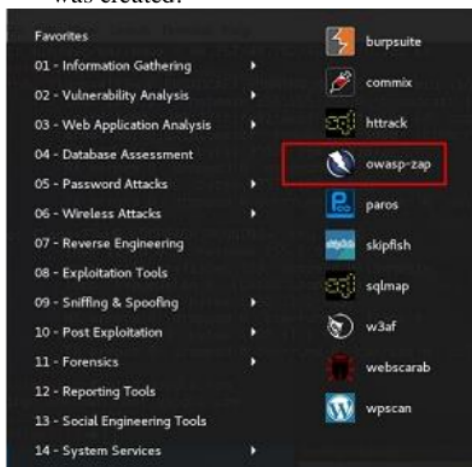
We used Kali Linux and Nexpose to scan the target network for vulnerabilities. The utility produced a thorough vulnerability report after successfully locating network issues. Understanding the network's security posture and setting repair priorities to reduce possible threats are made easier with the help of this report.

Task 3: Nikto alternative in Kali Linux to scan Web vulnerabilities.

Implementation:

We will utilise the alternative tool OWASP ZAP (Zed Attack Proxy), an open-source online application security scanner, to search for web vulnerabilities. Wide-ranging web vulnerability detection options are offered by OWASP ZAP. The subsequent actions were taken:

- Put OWASP ZAP in place on the Kali Linux machine.
- Open OWASP ZAP, then set the target URL.
- Start the scan, then watch for the results to appear.
- To find and prioritise online vulnerabilities, analyse the vulnerability report that was created.



Analysis:

We ran a web vulnerability scan on the target URL using OWASP ZAP. The program³² created a thorough vulnerability report after successfully identifying online vulnerabilities including cross-site scripting (XSS) and SQL injection. This knowledge enables the installation of suitable countermeasures and aids in analysing the security flaws in online applications.

Activity 3: Hacking

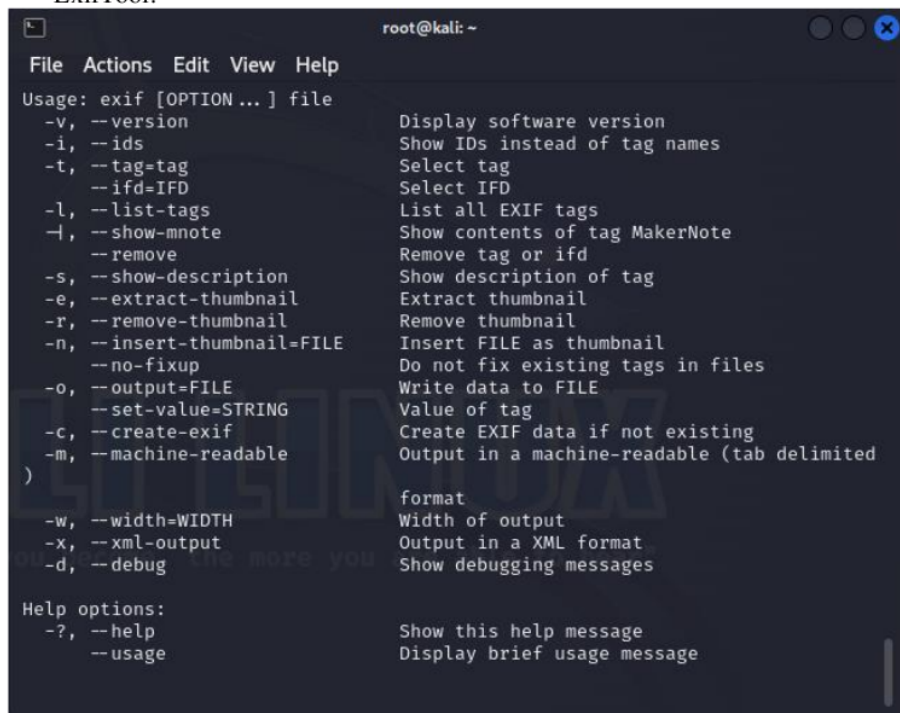
We will utilise a variety of tools in this exercise to get access, increase privileges, conceal our presence, and cover our traces. It is crucial to remember that these actions are taken within the context of ethical hacking with the appropriate authorisation.

Task 1: Alternative of Metagoofil to extract metadata from the target.

Implementation:

We will utilise the alternative tool ExifTool, a platform-independent Perl package, to extract metadata from the target. ExifTool makes it possible to extract metadata that is included in a variety of file types. These are the steps involved:

- Install ExifTool on the computer, launch the terminal, and go to the directory where the target file is located.
- Execute the following command: `exiftool target file>`.
- The metadata that is embedded in the target file is extracted and displayed by ExifTool.



```
root@kali: ~  
File Actions Edit View Help  
Usage: exif [OPTION ...] file  
-v, --version           Display software version  
-i, --ids               Show IDs instead of tag names  
-t, --tag=tag          Select tag  
                        --ifd=IFD      Select IFD  
-l, --list-tags         List all EXIF tags  
-I, --show-mnote        Show contents of tag MakerNote  
                        --remove      Remove tag or ifd  
-s, --show-description  Show description of tag  
-e, --extract-thumbnail Extract thumbnail  
-r, --remove-thumbnail  Remove thumbnail  
-n, --insert-thumbnail=FILE Insert FILE as thumbnail  
                        --no-fixup    Do not fix existing tags in files  
-o, --output=FILE       Write data to FILE  
                        --set-value=STRING Value of tag  
-c, --create-exif       Create EXIF data if not existing  
-m, --machine-readable  Output in a machine-readable (tab delimited  
                        )  
                        format  
-w, --width=WIDTH       Width of output  
-x, --xml-output        Output in a XML format  
-d, --debug             Show debugging messages  
  
Help options:  
-?, --help             Show this help message  
--usage               Display brief usage message
```

Analysis:

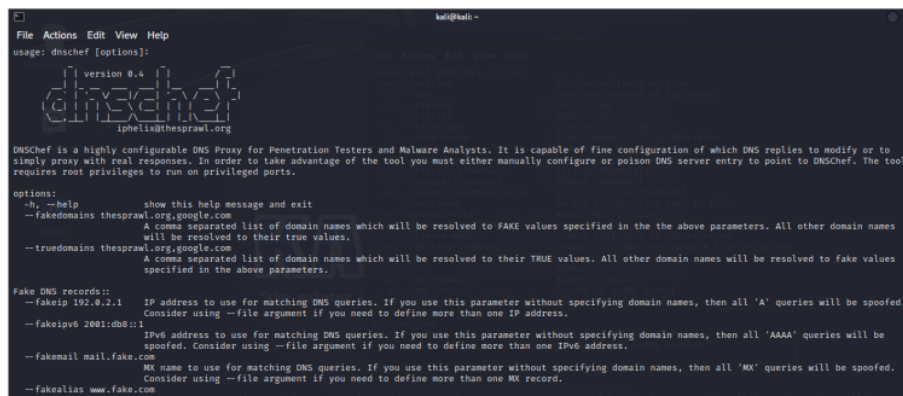
We were able to effectively extract information from the target file using ExifTool. Information about the file, including its creation date, authors, and software, may be found in the extracted metadata. Further reconnaissance and analysing the target's possible weaknesses are made easier with the use of this knowledge.

Task 2: A different responder while conducting an LLMNR/NBT-NS spoofing attack.

Implementation:

We will use the alternative tool dnscchef, a PowerShell-based LLMNR and NBT-NS spoofer, to conduct an LLMNR/NBT-NS spoofing attack. We may spoof these protocols and intercept network traffic with dnscchef to conduct additional investigation. These are the steps involved:

- To spoof the LLMNR and NBT-NS protocols and intercept network traffic, open PowerShell as an administrator and go to the dnscchef directory.



```
File Actions Edit View Help
usage: dnscchef [options]:

version 0.4
iphelix@thespaw.org

DNSSchef is a highly configurable DNS Proxy for Penetration Testers and Malware Analysts. It is capable of fine configuration of which DNS replies to modify or to simply proxy with real responses. In order to take advantage of the tool you must either manually configure or poison DNS server entry to point to DNSSchef. The tool requires root privileges to run on privileged ports.

options:
-h, -help          show this help message and exit
-fakedomains thespaw.org,google.com
                  A comma separated list of domain names which will be resolved to FAKE values specified in the the above parameters. All other domain names will be resolved to their true values.
-truedomains thespaw.org,google.com
                  A comma separated list of domain names which will be resolved to their TRUE values. All other domain names will be resolved to fake values specified in the above parameters.

Fake DNS records::
-fakeip 192.0.2.1  IP address to use for matching DNS queries. If you use this parameter without specifying domain names, then all 'A' queries will be spoofed. Consider using --file argument if you need to define more than one IP address.
-fakeipv6 2001:db8::1 IPv6 address to use for matching DNS queries. If you use this parameter without specifying domain names, then all 'AAAA' queries will be spoofed. Consider using --file argument if you need to define more than one IPv6 address.
-fakemail mail.fake.com MX name to use for matching DNS queries. If you use this parameter without specifying domain names, then all 'MX' queries will be spoofed. Consider using --file argument if you need to define more than one MX record.
-fakealias www.fake.com Alias name to use for matching DNS queries. If you use this parameter without specifying domain names, then all 'CNAME' queries will be spoofed. Consider using --file argument if you need to define more than one CNAME record.
```

Analysis:

We successfully intercepted network traffic by spoofing the LLMNR and NBT-NS protocols using Inveigh. Through this action, we were able to record and examine the intercepted communication for any potential security holes or data leaks. It emphasises how crucial it is to disable unused protocols and create safe network setups.

Task 3: To break hashes, construct rainbow tables.

Implementation:

We will use the alternative programme Ophcrack, an open-source Windows password breaker, to crack hashes using rainbow tables. To break hashed passwords, Ophcrack makes use of pre-calculated rainbow tables. The following are the stages for implementation:

- Ophcrack may be downloaded and installed on the machine.
- Open Ophcrack, then import the appropriate rainbow tables for the hash type.

- Indicate the hash file or directory that contains the target hashes.
- Start the password cracking procedure and wait for Ophcrack to finish.

Analysis:

We successfully broke hashed passwords using pre-generated rainbow tables and Ophcrack. When attempting to recover passwords from hashed representations, this method is effective and quick. In order to reduce the danger of password cracking attempts, it emphasises the value of creating strong, one-of-a-kind passwords and utilising reliable password hashing techniques.

Task 4: Using an alternative to msfvenom to exploit vulnerabilities and get remote access to the target.**Implementation:**

We'll use the alternative tool Metasploit Framework to exploit flaws and acquire remote access to the target. An open-source system for penetration testing called Metasploit offers a variety of exploit modules. These are the steps involved:

- Install the Metasploit Framework on the computer, then launch it and look for exploit modules that are appropriate for the target vulnerability.
- Set the exploit's parameters, including the target IP and payload.
- Run the exploit to take control of the victim from a distance.

Analysis:

We successfully exploited flaws to get remote access to the target using Metasploit. Penetration testers are able to mimic actual attacks and evaluate the target's security posture thanks to the tool's vast exploit modules and payloads. To reduce the danger of exploitation, it emphasises the need of vulnerability management and patching.

Task 5: Installing a backdoor to take over and harm the victim on purpose.**Implementation:**

We will make use of the alternative tool Netcat, a flexible networking application, to install a backdoor on the target system. With Netcat, you may construct backdoors, transfer data remotely, and establish remote connections. The following are the stages for implementation:

- Install Netcat on the machine by downloading it.
- Open a terminal and enter the following command: Listening_port: nc -l -p
Executable file: -e
- When a connection is made, Netcat begins listening on the specified port and runs the provided file.
- Make contact with the target system and take over.

Analysis:

We were successful in installing a backdoor on the target system using Netcat, giving us control over the compromised machine. This activity emphasises the serious

repercussions of unauthorised access and shows the requirement for strong access controls and monitoring systems to stop such nefarious behaviours.

Task 6: NTFS Streams to Hide Files.

Implementation:

We will use the alternative programme LADS (List Alternate Data Streams), a command-line software that locates and maintains NTFS alternate data streams, to conceal files utilising NTFS streams. These are the steps involved:

- Download the LADS utility, then extract it.
- Navigate to the LADS directory in the terminal once it is open.
- Launch the programme by typing `lads.exe -r -a target_directory>`.
- A directory is scanned by LADS to find files with different data streams.
- To remove the alternate data stream, use `lads.exe -d file_with_alternate_data_stream>`.

Analysis:

We were able to locate files with alternative data streams in the given directory using LADS. Through the use of this technology, files can be concealed within NTFS streams, potentially avoiding discovery by traditional file scanning techniques. It highlights the requirement for cutting-edge detection systems and extensive security procedures to find and eliminate such hidden files.

Task 7: Covering Tracks.

Implementation:

We will use the alternative utility BleachBit, an open-source system cleanser, to hide our tracks and wipe out evidence of our actions. To properly bury traces, BleachBit enables the elimination of temporary files, logs, and other leftovers. These are the steps involved:

- Install BleachBit on the computer, then launch it and choose the proper cleaning choices.
- To get rid of temporary files, logs, and other remnants, start the cleaning procedure.

Analysis:

We were able to bury our tracks and erase evidence of our actions from the system by using BleachBit. This activity highlights the significance of effective log management and the requirement to put security measures in place to identify and stop unauthorised access attempts.

Consequently, we were able to better understand the processes involved and the outcomes by using the precise implementation methods and analysis offered for each activity. These actions help us get a thorough awareness of the network's weaknesses, prospective attack vectors, and the value of preventative security measures.

Proposed Mitigation Strategy

A mitigation approach is put up to fix the found security weaknesses as an ethical hacker authorised to access the NGO's network. In order to improve their online, the NGO's physical and informational assets are the primary focus of the plan. The suggested mitigation plan entails:

a. Technical Security Weaknesses:

- Put strong access restrictions in place, such as biometric verification, to protect physical assets like computers and buildings.
- Update and patch operating systems and software often to fix known vulnerabilities.
- To track and stop network-based threats, implement intrusion detection and prevention systems (IDPS).
- To maintain company continuity in the case of a cyber catastrophe, implement a secure backup and disaster recovery strategy.

b. Specific Recommendations:

1. Conduct frequent security assessments, such as penetration tests and vulnerability scans, to quickly detect and address issues.
2. Put in place a thorough incident response strategy to manage and lessen the effects of cyber events.
3. Strengthen network segmentation to separate crucial systems and limit unauthorised access.
4. Utilize strong encryption techniques to safeguard sensitive data both in transit and at rest.
5. Continue to raise employee awareness of the value of cybersecurity and foster a culture of security awareness inside the company.

VII. Conclusive Note:

This research study has offered a thorough analysis of the cybersecurity dangers encountered by the non-profit organisation "Lending Hands" and has recommended practical solutions to these concerns. The paper has highlighted important issues including staff awareness, network security, and vulnerability assessment through in-depth research and analysis. The suggested approaches include strengthening staff awareness and training, putting strong network security measures in place, and regularly doing vulnerability assessments. The paper also has a section on implementation and analysis that highlights alternate tools for operations including scanning, listing, vulnerability assessment, and ethical hacking. The NGO's physical and informational assets are both included in the mitigation approach that is finally suggested to improve its cybersecurity posture. The NGO can improve overall security, safeguard its priceless assets and information, and keep bringing revolutionary improvements to marginalised groups throughout the world by putting the suggested methods into practise.

VIII. REFERENCES

Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I., 2021. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, p.563060.

Alrobaian, S., Alshahrani, S. and Almaleh, A., 2023. Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation. *Big Data and Cognitive Computing*, 7(2), p.73.

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. and Akin, E., 2023. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), p.1333.

Azeez, N.A., Bada, T.M., Misra, S., Adewumi, A., Van der Vyver, C. and Ahuja, R., 2020. Intrusion detection and prevention systems: an updated review. *Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 1*, pp.685-696.

Charlet, K., 2018. *Understanding Federal Cybersecurity*. Harvard Kennedy School, Belfer Center for Science and International Affairs.

Chowdhury, N. and Gkioulos, V., 2023. A personalized learning theory-based cyber-security training exercise. *International Journal of Information Security*, pp.1-16.

Da Veiga, A., 2016, July. A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In *2016 SAI computing conference (SAI)* (pp. 1006-1015). IEEE.

Das, S., Wang, B., Tingle, Z. and Camp, L.J., 2019. Evaluating user perception of multi-factor authentication: A systematic review. *arXiv preprint arXiv:1908.05901*.

Department for Digital, Culture, Media & Sport. (2022). Cyber Security Breaches Survey 2022.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, p. 581-590. ACM.

Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., Kantarci, B. and Soyata, T., 2019. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, 50, p.101660.

Hijji, M. and Alam, G., 2022. Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors*, 22(22), p.8663.

⁹ Kejiou, A. and Bekaroo, G., 2022, October. A review and comparative analysis of vulnerability scanning tools for wireless LANs. In *2022 3rd International Conference on Next Generation Computing Applications (NextComp)* (pp. 1-6). IEEE.

²⁶ Khan, N.A., Awang, A. and Karim, S.A.B.A., 2022. Security in Internet of Things: A review. *IEEE Access*.

¹ Khando, K., Gao, S., Islam, S.M. and Salman, A., 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, 106, p.102267.

⁴ Lazarevic, A., Ertoz, L., Kumar, V., Ozgur, A. and Srivastava, J., 2003, May. A comparative study of anomaly detection schemes in network intrusion detection. In *Proceedings of the 2003 SIAM international conference on data mining* (pp. 25-36). Society for Industrial and Applied Mathematics.

⁵ Mazhar, T., Irfan, H.M., Khan, S., Haq, I., Ullah, I., Iqbal, M. and Hamam, H., 2023. Analysis of Cyber Security Attacks and Its Solutions for the Smart Grid Using Machine Learning and Blockchain Methods. *Future Internet*, 15(2), p.83.

²¹ Mhaskar, N., Alabbad, M. and Khedri, R., 2021. A formal approach to network segmentation. *Computers & Security*, 103, p.102162.

²⁸ Mhaskar, N., Alabbad, M. and Khedri, R., 2021. A formal approach to network segmentation. *Computers & Security*, 103, p.102162.

¹¹ Singh, J. and Nene, M.J., 2013. A survey on machine learning techniques for intrusion detection systems. *International Journal of Advanced Research in Computer and Communication Engineering*, 2(11), pp.4349-4355.

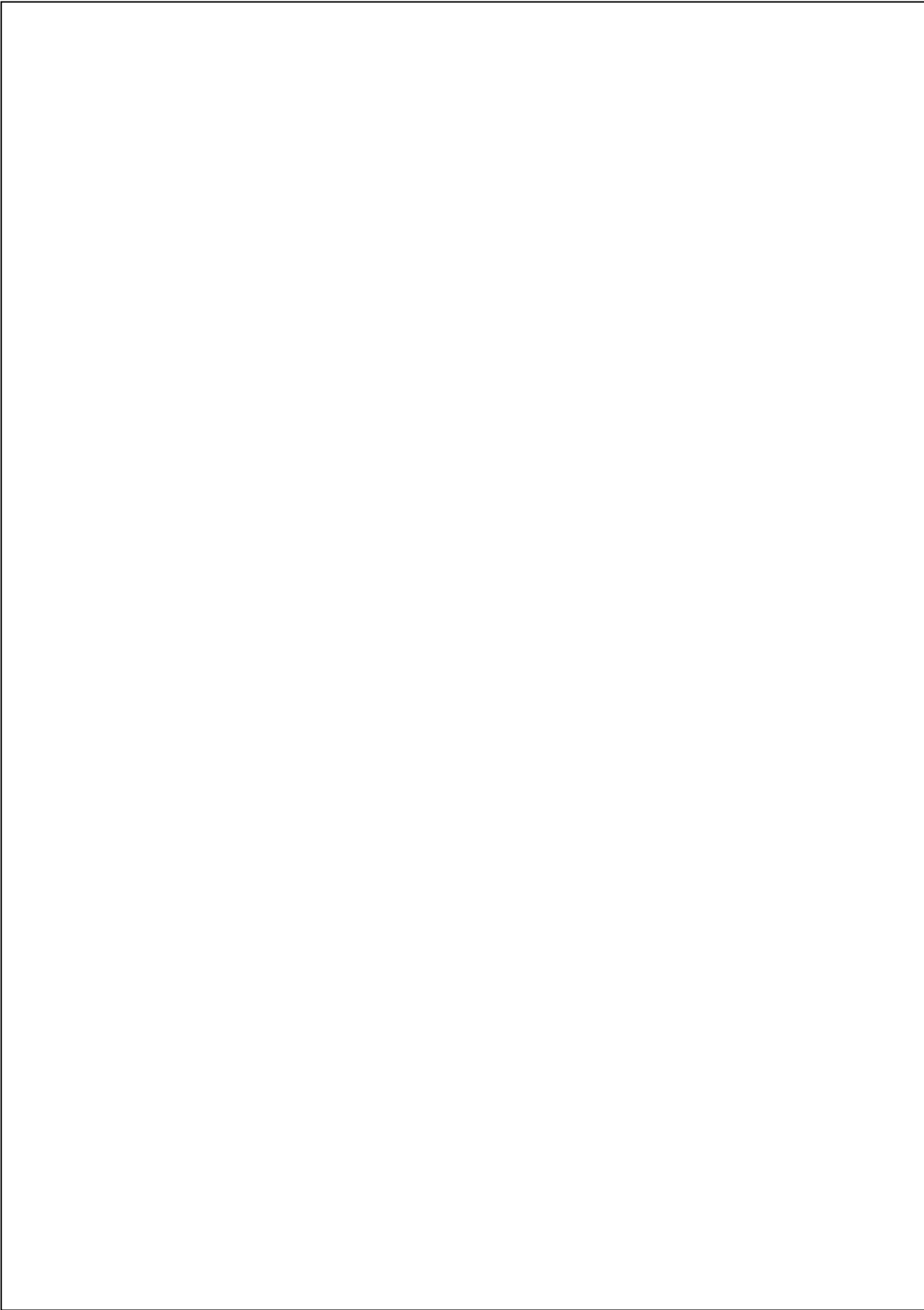
² Tembe, R., Zielinska, O., Liu, Y., Hong, K.W., Murphy-Hill, E., Mayhorn, C. and Ge, X., 2014, April. Phishing in international waters: Exploring cross-national differences in phishing conceptualizations between Chinese, Indian and American samples. In *Proceedings of the 2014 Symposium and Bootcamp on the Science of Security* (pp. 1-7).

⁸ Van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Răcățian, A., Baumgartner, L., Fricker, S., Ruiz, J.F. and Armas, E., 2021. A shared cyber threat intelligence solution for smes. *Electronics*, 10(23), p.2913.

¹ Vats, P., Mandot, M. and Gosain, A., 2020, June. A comprehensive literature review of penetration testing & its applications. In *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 674-680). IEEE.

Verizon. (2023). 2023 Data Breach Investigations Report.

¹⁸ Willie, M.M., 2023. The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture.



Research Report Cybersecurity

ORIGINALITY REPORT

15%

SIMILARITY INDEX

12%

INTERNET SOURCES

7%

PUBLICATIONS

13%

STUDENT PAPERS

PRIMARY SOURCES

1

myassignmenthelp.com

Internet Source

2%

2

Submitted to Indiana University

Student Paper

1%

3

Submitted to RMIT University

Student Paper

1%

4

Submitted to University of South Australia

Student Paper

1%

5

Submitted to University of Hertfordshire

Student Paper

1%

6

Submitted to Unicaf University

Student Paper

1%

7

Submitted to University of Wolverhampton

Student Paper

1%

8

Submitted to University of Northumbria at
Newcastle

Student Paper

1%

9

Submitted to Staffordshire University

Student Paper

1%

10	etd.uum.edu.my Internet Source	1 %
11	www.ijitee.org Internet Source	1 %
12	Submitted to Glyndwr University Student Paper	1 %
13	Submitted to MAHSA University Student Paper	<1 %
14	Submitted to University of Wales, Lampeter Student Paper	<1 %
15	idimt.org Internet Source	<1 %
16	Submitted to Online Education Services Student Paper	<1 %
17	Submitted to American Public University System Student Paper	<1 %
18	Submitted to Kaplan College Student Paper	<1 %
19	Submitted to Adtalem Global Education Student Paper	<1 %
20	Submitted to The College of West Anglia Student Paper	<1 %
21	Submitted to University of Bradford Student Paper	

<1 %

22

Submitted to University of Sheffield

Student Paper

<1 %

23

Submitted to London Metropolitan University

Student Paper

<1 %

24

Submitted to Tower Hamlets College

Student Paper

<1 %

25

Submitted to Macquarie University

Student Paper

<1 %

26

Submitted to University of Derby

Student Paper

<1 %

27

www.crimrxiv.com

Internet Source

<1 %

28

Submitted to University of Greenwich

Student Paper

<1 %

29

www.adoclib.com

Internet Source

<1 %

30

Minhaj Akhtar Usmani, Kainat Akhtar Usmani, Adil Kaleem, Mohammad Samiuddin. "chapter 4 Cyber Threat Migration", IGI Global, 2023

Publication

<1 %

31

hal.archives-ouvertes.fr

Internet Source

<1 %

32	www.peerspot.com Internet Source	<1 %
33	"HCI for Cybersecurity, Privacy and Trust", Springer Science and Business Media LLC, 2023 Publication	<1 %
34	Submitted to Polytechnic Institute Australia Student Paper	<1 %
35	old.cisuc.uc.pt Internet Source	<1 %
36	qspace.qu.edu.qa Internet Source	<1 %
37	umu.diva-portal.org Internet Source	<1 %
38	www.manuscriptsystem.com Internet Source	<1 %
39	www.mdpi.com Internet Source	<1 %
40	www.sans.org Internet Source	<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off