



University of East London

Pioneering Futures Since 1898
School of Architecture, Computing and Engineering

Module code: CN7014 2324 (T1)

Module Title: Security Management (OC)

Module Leader: Dr. Umar Ismail
Moses Bankole, Dr Halima Kure, Dr Shazad Memon.

Data Breach Title: Marriott International Starwood 2018
Case Study: Marriott International Starwood 2018

BY:

PHYLLIS JEBICHII ROP - U2707571
SAURAV GURUNG - U2773653

Table of Content

Abstract	3
Introduction	4
Task 1: Security Incident and Threat Intelligence	5
1.1 Incident Details.....	5
1.1.1 Date of the incident.....	5
1.1.2 Incident type	5
1.1.3 Summary of the incident.....	5
1.1.4 System Compromised.....	5
1.1.5 Data compromised.....	5
1.1.6 Approximate number of users affected.....	5
1.1.7 Number of sites affected	5
1.1.8 System Compromised.....	5
1.1.9 Data compromised.....	6
1.1.10 Approximate number of users affected.....	6
1.1.11 Number of sites affected	6
1.2 Incident Analysis	6
1.2.1 Causes of the Incident.....	6
1.2.2 Method of Incursion	7
1.2.3 Incident Duration.....	7
1.2.4 Origin of the incident.....	7
1.2.5 Size/percentage of the organization systems affected.....	7
1.2.6 Estimated current and potential technical effect of the incident	7
1.2.7 Estimated current and potential legal and regulatory impact of the incident	7
1.3 Cyber Threat Intelligence Analysis	8
1.3.1 Threat Actor Skill and Motivation.....	8
1.3.2 Indicator of Compromise.....	8
1.3.3 Exploited vulnerabilities.....	8
1.3.4 Tactics, Techniques and Procedure (TTP) of the attacker	8
1.3.5 Access vector of the attack	8
1.4 Controls	8
1.4.1 Steps taken.....	9
1.4.2 Who was notified after the incident?	9
1.4.3 Response strategies.....	9
1.4.4 Recommended Control Actions	10
Task 2: Automated Vulnerability Scanning and Analysis	10
2.1 How many vulnerabilities item did you find?.....	13
2.2 What are Common Vulnerabilities and Exposures (CVE)?.....	13
2.3 Two Vulnerabilities	16
Task 3: Information Security Risk Assessment and Management	17
3.1 Inventory of Assets.....	18
3.2 Risk Register	19
3.3 Risk control	21
Task 4: Incident Response.....	22
4.1 Preparation.....	22
4.1.1 Purpose:.....	22
4.1.2 Scope:	22
4.1.3 CSIRT Team	23
4.1.3.1 CSIRT Type	23
4.1.3.2 CSIRT Member Type	23
4.1.3.3 Skills and Abilities	23
4.1.3.4 Assign Roles and Responsibilities	23

4.2 Detection and Analysis	2	3
4.2.1 Detection Strategies to be used:	2	4
4.2.2 Attack Vectors to Consider	2	4
4.2.3 Data Categories/Types of Data to Collect:	2	4
4.2.4 Source of the Data:	2	4
4.2.5 Prioritization of incidents	2	5
4.3 Containment, Eradication and Recovery	2	5
4.3.1 Containment Measure and Description.....	2	5
4.3.2 Eradication Measure and Description.....	2	6
4.3.3 Recover Measure and Description	2	6
Self-Reflection.....	2	7
Presentation Slides	2	9
References	3	3

Table of Tables

Table 1 Inventory of Assets..... 1 8

Table 2 Risk Register 2 0

Table 3 Risk Controls..... 2 2

Table of Figures

Figure 1 Open ports scanned from Nmap.....	1	1
Figure 2 Nessus installation.....	1	2
Figure 3 Total number of vulnerabilities scanned from Nessus	1	3
Figure 4 Slide 1	2	9
Figure 5 Slide 2	2	9
Figure 6 Slide 3	3	0
Figure 7 Slide 4	3	0
Figure 8 Slide 5	3	1
Figure 9 Slide 6	3	1
Figure 10 Slide 7	3	2
Figure 11 Slide 8	3	2

Abstract

Marriott International is a renowned global hospitality company founded in Bethesda, Maryland, USA. It was started in 1927 by J. Willard Marriott and his wife Alice Marriott as a root beer stand. Over the years, Marriott has grown to be a reputable hotel industry with approximately 8,700 properties under 30 distinct brands across 139 countries as of 2024. The company's brand consists of luxury, premium and select service accommodation owning popular hotels like Ritz-Carlton, JW Marriott, Sheraton, and W Hotels. (Marriott Announces Starwood Guest Reservation Database Security Incident, 2018)

In 2016 Marriott made a big purchase of Starwood hotel and resort and integrated into its daily business operations. This purchase later contributed to the massive data breach identified in November 2018 that led to unauthorized access of approximately 500 million customers' data including names, contact information, passport details and payment details. The data breach caused a lot of doubts towards Marriott's cybersecurity strategy's acquisition process and protection towards its customers' data from unauthorized persons. The incident caused Marriott's financial reputation and legal action including fines and lawsuits.

Introduction

On this task, we will be looking into the Marriott International data breach that was flagged in September 2018 due to unusual activities and how the attack affected the guest reservation database that housed Starwood brands such as Westin, Sheraton, St. Regis and W Hotels. We will have comprehensive information coverage on the breach from the details on the incident highlighting when it occurred, the type of data that was compromised and a detailed summary covering the incident. The task will also classify the incident based on how sensitive it was and the degree of exposure to its users.

A research analysis on the contribution towards the weaknesses in the network and system design that contributed to the breach occurrence will be covered. Details on the type of network, operating system and malicious code that contributed to the violation will also be highlighted. We will also talk about the ways attackers got into the system, how long they were there, and where the intrusion came from. The study will look at how big the organization that was affected is, what the present and possible technical effects are, and what the legal and regulatory effects of the event are.

The report will evaluate the threat landscape displaying how the attackers were able employ their skills and what motivated them to access the Starwood system. Exploited vulnerabilities and methods used for the attack, with tactics, techniques, and procedures (TTPs) used will be addressed. Lastly, the control action implemented covering the containment, eradication and recovery used to restore the services of Marriott International and future steps towards improving security defense from potential attacks.

Task 1: Security Incident and Threat Intelligence

1.1 Incident Details

1.1.1 Date of the incident

The Marriott International breach was discovered on 8th September 2018 when an internal security tool flagged unauthorized access attempt to the Starwood guest reservation database. However, this intrusion had been ongoing since 2014 before Marriott bought Starwood in 2016. The breach was then publicly disclosed on 30th November 2018. (Denuwan, 2023)

1.1.2 Incident type

This was a data breach incident involving unauthorized access to the Starwood guest reservation database. The attack exploited vulnerabilities in the legacy Starwood systems.

1.1.3 Summary of the incident

Marriott discovered that hackers had been accessing and ex-filtrating encrypted guest data from the Starwood reservation system. The breach had already occurred before Marriott acquired Starwood and failed to conduct proper integration of the system before using it and secure Starwood's IT infrastructure. The attackers were able to copy, encrypt and remove sensitive data from the database that contains sensitive client's data.

The unauthorized accessed data was very sensitive and confidential. It included:

- Names
- Mailing addresses
- Phone numbers
- Email addresses
- Passport numbers
- Starwood Preferred Guest account information
- Dates of birth
- Gender
- Arrival and departure dates
- Reservation details
- Encrypted payment card information (Marriott Announces Starwood Guest Reservation Database Security Incident, 2024)

1.1.4 System Compromised

The Starwood guest reservation database was compromised. This system had outdated and vulnerable IT infrastructure, which facilitated the breach.

1.1.5 Data compromised

Approximately 500 million customer records were exposed. Among these, about 327 million records contained detailed sensitive information.

1.1.6 Approximate number of users affected

An estimated 500 million users globally were affected, although this includes duplicate records

1.1.7 Number of sites affected

The breach impacted all Starwood branded properties, including notable brands like W Hotels, Sheraton, St. Regis, Westin and more across multiple countries

1.1.8 System Compromised

The Starwood guest reservation database was compromised. This system had outdated and vulnerable IT infrastructure, which facilitated the breach.

1.1.9 Data compromised

Approximately 500 million customer records were exposed. Among these, about 327 million records contained detailed sensitive information.

1.1.10 Approximate number of users affected

An estimated 500 million users globally were affected, although this includes duplicate records

1.1.11 Number of sites affected

Although specific number of sites affected were not mentioned, the breach impacted all Starwood branded properties, including notable brands like W Hotels, Sheraton, St. Regis, Westin and more across multiple countries.

1.2 Incident Analysis

Analyzing Marriott International's data breach provides key to understanding the specific perceptions regarding modern cybersecurity incidents. This analysis highlights major security gaps, Marriott's response to mitigate risks, and the importance of stronger data protection, especially in organization mergers. It underscores the enhanced cybersecurity requirement to rebuild customer's trust and prevent future breaches.

1.2.1 Causes of the Incident

Network

Malicious Code: The breach involved continuous unauthorized access to Starwood's guest reservation system, which was facilitated by advanced malicious code and tool. The attacker penetrated the Starwood network in 2014 using a web shell. Then, they used Remote Access Trojan (RAT) and Mimikatz, a tool that extracts usernames and passwords from system memory, but such Trojans are often downloaded from phishing emails. It is believed that combination of these two tools could have given full access control of administrator account to the attackers Josh (2020).

Access Violation: The breach highlighted a critical access violation, revealing weak security protocols that could not protect the organization's network. The attackers successfully bypassed Starwood's access control which indicates weakness in the network's authentication and authorization mechanism.

Accidental Error: The breach could have been successful due to lack of proper security configuration on all systems or networks or could have missed any security patches which laid the entire Starwood's infrastructure vulnerable. We can make assumption that the organization lacked implementation of proper access controls, neglected time-to-time security patches, lack of strict security monitoring system or failed to notice multi-factor authentication on every high priority system which could have left the systems vulnerable. This also reflects possible human errors in not maintaining secured security protocols which contributed to the attack successful and undetectable for long period of time.

Systems

Type of Network: The Starwood guest reservation database was the type of network affected. The database holds millions of critical, sensitive and confidential information which made it the most appropriate target for the attackers.

Operating System: The operating system details of the compromised systems are not disclosed by Marriott International but there are many reputable sources assuming that Windows-based servers are commonly used in hotel chains like Marriott. The outdated versions of Windows server likely contributed to the vulnerabilities that were exploited in the breach.

Protocols/Services: There is no specific protocols and services involved in the hacked network or system clearly published to public however, understanding these protocols and

services would help to identify the weak entry areas which could help to improve the security and prevent from any similar kind of data breaches or cyber-attacks in future.

Application: Starwood guest reservation is the application affected by the incident. The reservation system exposed millions of raw sensitive data like names, mailing address, contact details, email address, passport details, Starwood Preferred Guest account information, date of birth, arrival/departure details and encrypted payment card details of the customers to the attackers. (Amanulla and Niyaz, 2024) Marriott has not provided the information regarding the access of attackers on decryption keys.

1.2.2 Method of Incursion

The method of incursion in the Starwood guest reservation database breach involved a complex attack that allowed unauthorized access to the network, likely through use of malware but is not clearly published to the public. The attackers were successful in bypassing the security measures, copying and encrypting the information. There are no specific details regarding the method of the attack and this breach highlights the need for detailed forensic analysis.

1.2.3 Incident Duration

The duration of the Marriott International data breach lasted about four years. On September 8, 2018, there was a first alert received and on November 19, 2018, they were able to discover the compromised data. On November 30, 2018, Marriott released a statement regarding to the public mentioning unauthorized access to the network since 2014.

1.2.4 Origin of the incident

The exact origin of the Marriott International data breach remains unclear as Marriott has not disclosed any specific technical details such as any attacker's source IP addresses or targeted IP address, port details or chance of any malware entry point.

1.2.5 Size/percentage of the organization systems affected

The Starwood network was completely hacked during the data breach, affecting all the systems linked to its reservation platform. However, Marriott has not shared exact details about how much of its larger network was impacted after the merger. The lack of detailed public information creates room for assumptions about the breach's full impact.

1.2.6 Estimated current and potential technical effect of the incident

However, the Marriott has mentioned that payment card details and certain passport numbers of data on the compromised database were encrypted with AES128 encryption method and SHA1 cryptography encryption respectively, there is also the chance of potentials compromise of the encryption key in the same network server which could enable attackers to decrypt and misuse the sensitive information, posing a significant risk to affected individuals.

1.2.7 Estimated current and potential legal and regulatory impact of the incident

Marriott was initially fined £99.2 million by the UK's Information Commissioner's Office (ICO) for failing to meet GDPR security standard. But, after considering different mitigating factors like economic impact of covid-19, cooperation with authorities, limited financial harm, and more the fine was reduced to £18.4 million. ('Marriott International Inc, Penalty Notice - 30 October 2020', no date) The exact date of payment has not been disclosed to the public, but Marriott chose not to appeal, which indicates that the fine amount has been settled.

In conclusion, the incident analysis of the Marriott International data breach reveals significant vulnerabilities in the network security, access controls and security practices particularly after the merger acquisition with Starwood. The infrastructure was outdated, illegal access remained unnoticed for four years and the system monitoring was insufficient, so almost 500 million client data were compromised. This breach demonstrates the reasons hotel-industry like Marriott should develop their infrastructure at top level, enhance their digital security and closely monitor the access activities of sensitive data. They also must

consider the financial and legal circumstances of GDPR or brand reputation harm. Making the customer's confidence in their brand and preventing any such future cyber-attacks depends on first giving customer data high priority.

1.3 Cyber Threat Intelligence Analysis

The analysis of the cyber threat intelligence surrounding the Marriott data breach involves a deep dive into the motivations, skills, and tactics employed by the threat actor. We will cover indicators leading to the compromise that allowed the system's weaknesses to be exploited, and methods used to achieve the attack.

1.3.1 Threat Actor Skill and Motivation

The threat actors behind the breach were highly skilled using Advanced Persistent Threat (APT) techniques. The skilled used to access Starwood guest reservation database demonstrated how sophisticated the attackers were with their highly acquired skills. They were able to maintain unauthorized entry into the Starwood system from 2014 before Marriott acquired Starwood in 2016 to November 2018 when they were discovered. The motivation behind the attack appears to be a blend of data exploitation and financial gain from the encrypted customers payment card details. The extensive nature of the attack, having lasted for approximately 4 years, shows how the threat actors had a strategic long-term approach towards the data acquired.

1.3.2 Indicator of Compromise

Indicators included unusual, encrypted data ex-filtration, unauthorized access logs in Starwood's reservation system, and malicious code embedded within the database servers to extract customer information.

1.3.3 Exploited vulnerabilities.

The breach exploited long standing vulnerabilities in Starwood's legacy IT systems, such as inadequate encryption practices, poor segmentation of sensitive data, and weak authentication protocols for critical systems.

1.3.4 Tactics, Techniques and Procedure (TTP) of the attacker

The attackers demonstrated skillful Tactics, Techniques and Procedures to access Starwood system. This includes.

- Spear Phishing to gain unauthorized access to Starwood network.
- Credential Dumping to elevate their chances and privileges within the network.
- Deployment of custom malware to maintain persistence and using used Remote Access Trojan (RAT) and Mimikatz.
- Data Ex-filtration via encrypted outbound traffic channels where attackers copied and tried to encrypt gathered data.

1.3.5 Access vector of the attack

It is yet unknown exactly how the threat actors got access to Starwood however, understanding how the attackers broke in the network and started the breach depends on knowing the access vector. Perhaps by means of spear phishing emails or other social engineering techniques, the attackers may have acquired access by means of exploiting vulnerabilities in the network system using compromised credentials. Before Starwood was bought and included into Marriott international system, this gave access to their weakly guarded network. The breach clearly highlighted the importance of maintaining rigorous cybersecurity practices by patching management and comprehensive security audits during acquisitions processes.

1.4 Controls

1.4.1 Steps taken

After the data breach, Marriott International took the steps mentioned below and response strategies to solve the root cause of the event, minimize the impact and improve the cyber security measures.

The steps taken to mitigate the incident are:

1. Incident Response Plan: Marriott International prepared an immediate incident response plan which allowed them to respond to the breach. This includes a team of experts who started internal investigation after detecting the alert in the Starwood network which identified the unauthorized access of unknown party undetected since 2014.
2. Notified respective law enforcement: Marriott reported the data breach to law enforcement like ICO and FBI and worked closely with them with full collaboration for further forensic investigation.
3. Customer Notification: Marriott officially notified about data breach to their customers through different strategies like press release, website notifications, and direct contacting to affected customers. The organization also set up a call center to address customers' concerns. They offered affected customers of UK, USA and Canada a free identity protection and credit monitoring subscription to Web-watcher for one year to help to protect against any possible fraud. They also agreed to pay for passport replacement for customers who were victimized of any fraud.
4. Technical Measures and improving security: Marriott International implemented several technological actions like password re-initialization, enhancement of system security and proper system monitoring mechanisms to detect and prevent future attacks effectively.

1.4.2 Who was notified after the incident?

As soon as Marriott believed their data breach, firstly they reached law enforcement and regulatory bodies. After that, Marriott tried to reach out to their affected customers with a dedicated support line for any fraud assistance. They also disclosed information regarding their valuable customer's data breach with the public which built transparency and trust to their customers as they were providing updates regarding the incident.

1.4.3 Response strategies

Marriott International has not shared any specific details of their forensic investigation with their stakeholders. However, they should have had an incident response plan to address data breach focusing on containment, eradication and system recovery.

1. Containment

Immediate Isolation: Marriott separated the compromised systems from other systems on infrastructure to stop any further unauthorized access and prevent additional leakage of data.

Incident Assessment: A dedicated team of cybersecurity professionals was brought in to determine the extent of the breach and identify which systems were affected.

Monitoring and Alerts: Advanced monitoring tools were implemented to identify and prevent any continuing malicious activities.

2. Eradication

Removal of Malicious Code: Advanced malware and tools like the Remote Access Trojan (RAT) and Mimikatz were identified and removed from the organization's network.

Patching Vulnerabilities: Marriott applied security patches and updated software to address exploited vulnerabilities in the network and systems.

Revoking Access: Compromised accounts should have been disabled, and access permissions were re-evaluated to prevent from any further misuse.

3. Recovery

System Restoration: Affected systems were restored and isolated from any real time enterprise network.

Improved Security measures: Marriott began changing the Bonvoy account passwords for every client. For high priority systems, they also kept improving encryption technologies, appropriate access restrictions and implementing multi-factor authentication.

Customer transparency: Marriott notified all the affected customers regarding their data breach.

Collaboration with Authorities: Marriott teamed up with police and government officials to investigate the incident and follow all the necessary legal rules.

1.4.4 Recommended Control Actions

There are different recommended controls reflecting preventive, technical and administrative controls.

1. Preventive controls

- **Proper data encryption**
The risk of data theft can be considerably reduced by making sure that sensitive data are encrypted while it is in transit and at rest. Marriott could have mitigated the impact of the breach by enhancing their encryption procedures for all payment information and personally identifiable information (PII).
- **Multi-factor authentication (MFA)**
All privileged access accounts and customer-facing services should have been subject to MFA, which would have made it more difficult for hackers to obtain unauthorized access. MFA could add one layer of security for hackers to use stolen credentials.

2. Technical Controls

- **Real-time monitoring and intrusion detection system**
It may be possible to detect intrusions faster by using sophisticated threat detection systems that combine AI and machine learning to recognize abnormal network behavior. Marriott would be able to identify threats as the system would identify the affected system which could reduce damage and speed up the reaction times.
- **Proper Network segmentation**
Marriott could have implemented stricter network segmentation like creating VLANs especially between public facing servers and the reservation system. This would have limited the attacker's ability inside the infrastructure.

3. Administrative controls

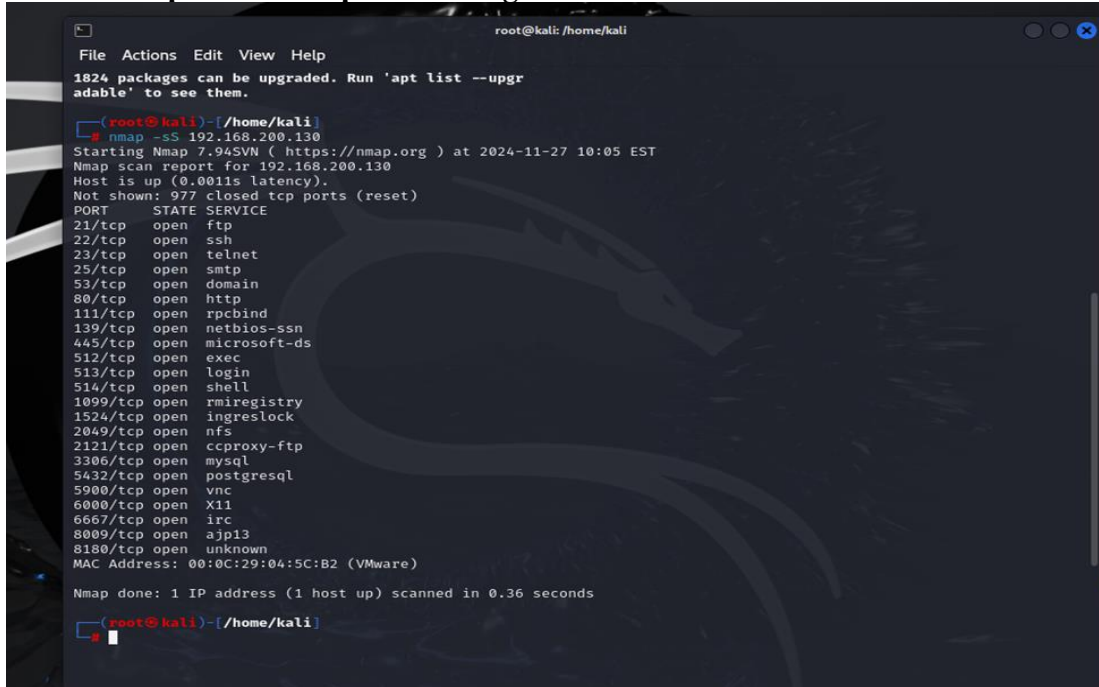
- **Staff training and awareness**
Regular security awareness training for all employees might assist in avoiding social engineering attacks like phishing, which are most likely used in this type of cyber-attacks. Educating employees on the best enterprise level practices and emerging risks ensures that they can act as an initial security layer.
- **Access control policies**
Marriott should have implemented an even more strict access control policy, ensuring only authorized user access to the information required for their function. Role-based access control (RBAC) could have been mitigating the likelihood of internal threats or compromised users accessing critical systems.

Task 2: Automated Vulnerability Scanning and Analysis

In task2, a virtual machine image called Metasploitable was provided to us, and we opened the image on VMware. The operating system used for scanning the vulnerabilities in the

provided machine was Kali GNU/Linux rolling version 2024.4. The IP Address for the target machine is 192.168.200.130. Kali Linux is also on the same network. The first step of Network Enumeration was port scanning of target machine using Nmap tool. Nmap (Network Mapper) is an open-source Linux network scanning and reconnaissance tool used to scan IP Address and ports in a network. It is designed to discover hosts, services and vulnerabilities on any network quickly. (John Breeden II, 2022)

The list of open services/ports on target machine.



```
root@kali: /home/kali
File Actions Edit View Help
1824 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@kali: /home/kali
# nmap -sS 192.168.200.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 10:05 EST
Nmap scan report for 192.168.200.130
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:04:5C:B2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
root@kali: /home/kali
```

Figure 1 Open ports scanned from Nmap

Installation of Nessus

Downloaded Nessus using curl command.

```
curl --request GET \ --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.8.3-x64.msi' \ --output 'Nessus-10.8.3-x64.msi'
```

```
(kali@kali)-[~]
$ sudo dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 410999 files and directories currently installed.)
Preparing to unpack Nessus-10.8.3-ubuntu1604_amd64.deb ...
Unpacking nessus (10.8.3) ...
Setting up nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KDKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.servic
e
- Then go to https://kali:8834/ to configure your scanner
```

Figure 2 Nessus installation

After a complete scan, Nessus provided the full report where we identified five levels of vulnerability severity on the target machine. The severity of a vulnerability refers to the possible damage it could cause to a system if someone takes access to it. This helps to decide the organization how urgently it should be fixed. Vulnerabilities are ranked on how much harm they could cause and how likely they are to be exploited.

CVSS is a scoring system that ranks computer system vulnerabilities on a scale of 0 to 10, with 10 representing the most serious. These scoring are used to categorize vulnerabilities into five severity categories, allowing security actions to be prioritized more effectively.

- **Critical Severity**
These vulnerabilities are the most serious and simplest to exploit, which allow attackers to take over victim's machine totally. The system administrator or user are advised to patch or update the system urgently. The CVSS score for this vulnerability is between 9 to 10.
- **High Severity**
These vulnerabilities are although difficult to exploit, they are still harmful and may result in major issues like system failures or data breaches. For these kinds of vulnerabilities, it is advised that significant upgrades be applied as soon as possible. The CVSS score for this vulnerability is between 7 to 8.9.

- **Medium Severity**
These vulnerabilities require that attackers to be on same local network with victim and may also use social engineering to exploit. For these kinds of vulnerabilities, user must apply the security patches of the system. The CVSS score for these vulnerabilities is between 4.0 to 6.9.
- **Low Severity**
These vulnerabilities have less effect and require frequent involvement of physical access of the attackers to success the exploit. The patches should be applied only if it is necessary. The CVSS score of these kinds of vulnerabilities is between 0.1 to 3.9. (Han, Li, Xing, Liu, Feng, 2017)
- **Informational**
In this level, there is not any direct security risk, but however it offers useful information like version or configuration details of any program. There is no CVSS score for this level.

2.1 How many vulnerabilities item did you find?

Critical: Number of critical-severity vulnerabilities discovered

10

High: Number of high-severity vulnerabilities discovered.

7

Medium: Number of medium-severity vulnerabilities discovered.

26

Low: Number of low-severity vulnerabilities discovered.

9

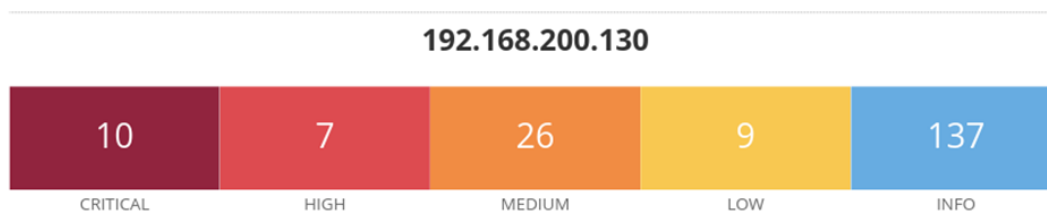


Figure 3 Total number of vulnerabilities scanned from Nessus

2.2 What are Common Vulnerabilities and Exposures (CVE)?

CVE-2020-1745

Affected Software/Component: Apache Tomcat AJP Connector.

Nature of the Vulnerability: File inclusion vulnerability enabling attackers to access arbitrary files or execute malicious code remotely.

CVSS Score: 9.8 (Critical)

CVE-2008-0166

Affected Software/Component: Debian OpenSSL

Nature of Vulnerability: The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. ("Debian OpenSSH/OpenSSL Package Random Number Generator Weakness ...") An attacker can easily obtain the private part of the remote key and use it to setup decipher the remote session or able to do Man-In-The-Middle attack.

CVSS Score: 10 (Critical)

CVE-2010-2075

Affected Software/Component: UnrealIRCd (3.2.8.1)

Nature of Vulnerability: A malicious backdoor was injected into the source code of UnrealIRCd which allowed attackers to execute arbitrary command on the affected server without authentication.

CVSS Score: 10(Critical)

CVE-2008-0166

Affected Software/Component: Debian OpenSSL.

Nature of the Vulnerability: Weak random number generation allows attackers to predict cryptographic keys, leading to data compromise.

CVSS Score: 7.8 (High)

CVE-2010-2075

Affected Software/Component: UnrealIRCd (Internet Relay Chat Daemon).

Nature of the vulnerability: This vulnerability is due to a backdoor in certain versions of UnrealIRCd. The backdoor allows attackers to execute arbitrary commands with the privileges of the affected server, leading to full system compromise.

CVSS Score: 7.5 (High)

CVE-2020-8616

Affected Software/Component: ISC BIND 9

Nature of the vulnerability: A flaw in BIND's handling of DNS delegation responses allows an attacker to exploit a logic error. This can trigger a condition leading to a crash of the BIND server, causing a Denial of Service (DoS).

CVSS Score: 8.6 (High)

CVE-2016-2183

Affected Software/Component: SSL/TLS Protocols (SWEET32 Vulnerability).

Nature of the Vulnerability: Exploitation of 64-bit block ciphers like 3DES allows attackers to recover plaintext from encrypted traffic.

CVSS Score: 5.3 (Medium).

CVE-2016-2118

Affected Software/Component: Samba.

Nature of the Vulnerability: Authentication flaws allow privilege escalation and potential exposure of sensitive data.

CVSS Score: 7.1 (High).

CVE-1999-0651

Affected Software/Component: rlogin/rsh Services.

Nature of the Vulnerability: Use of cleartext protocols allows attackers to intercept sensitive information or execute unauthorized commands.

CVSS Score: 7.5 (High).

CVE-2014-3566

Affected Software/Component: SSLv3 Protocol (POODLE Vulnerability)

Nature of the Vulnerability: A man-in-the-middle attacker can exploit SSLv3's padding mechanisms to decrypt sensitive information from encrypted communications.

CVSS Score: 4.3 (Medium).

CVE-2020-8617

Affected Software/Component: ISC BIND DNS Server.

Nature of the Vulnerability: Improper handling of specific DNS responses may cause a server crash, resulting in a Denial of Service (DoS)

CVSS Score: 6.8 (Medium).

CVE-2008-1447

Affected Software/Component: DNS Protocol

Nature of vulnerability: The remote DNS resolver does not use random ports when making queries to third-party DNS servers. "An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites." ("Multiple Vendor DNS Query ID Field Prediction Cache Poisoning")

CVSS Score: 6.8 (Medium)

CVE-2007-1858

Affected Software/Component: SSL protocols

Nature of vulnerability: The remote host supports the use of anonymous SSL ciphers. "While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack." ("SSL Anonymous Cipher Suites Supported - Tenable")

CVSS Score: 5.9(Medium)

CVE-2016-0800

Affected Software/Component: OpenSSL(V2)

Nature of vulnerability: protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened encryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key. ("SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete a...")

CVSS Score: 5.9(Medium)

CVE-2003-1567

Affected Software/Component: Apache HTTP Server, Microsoft IIS and Sun Java System Web Server

Nature of Vulnerability: An attacker can exploit HTTP TRACE and HTTP TRACK methods which are used for debugging purposes to perform a cross-site-tracing (XST) attack. Malicious script executed in the victim's browser interacts with the web server to expose the user's authentication tokens, cookies and other sensitive information.

CVSS Score: 5.8 (Medium)

CVE-2020-8622

Affected Software/Component: ISC BIND (9.11.21, 9.16.5, 9.17.3)

Nature of Vulnerability: Attackers can trigger an assertion failure which can cause the DBS server to crash or malfunction resulting in Denial of Service (DoS).

CVSS Score: 6.5(Medium)

CVE-2013-2566

Affected Software/Component: RC4 algorithm weakness in SSL/TLS Protocol

Nature of Vulnerability: The RC4 cipher encrypts data which can be predictable or biases. Attackers can easily exploit these patterns to decrypt raw information which could be passwords or any other personal details.

CVSS Score: 5.9 (Medium)

CVE-2008-5161

Affected Software/Component: SSH Protocol using block ciphers in Cipher Block Chaining (CBC) mode for encryption

Nature of Vulnerability: An attacker who is monitoring encrypted SSH traffic can manipulate the data stream and analyze responses from client to server and vice versa. This can allow the attacker to recover partial plain text data.

CVSS Score: 2.6 (Low)

2.3 Two Vulnerabilities

CVE-2016-2183 also known as SWEET32 vulnerability, is the flaw found in using DES/3DES cipher in SSL/TLS, SSH and IPSec protocols. Due to the small block size of 64 bits, the attackers can recover plaintext data by observing large amount of encrypted traffic on network.

Impact on the system

- An attacker could be able to decrypt sensitive information such as session cookies, login credentials or any payment details which are encrypted on the network.
- This vulnerability is a serious security risk as it compromises encrypted communications. It is dangerous for the systems using 3DES as a backup cipher in SSL/TLS. This vulnerability made the attacker access unauthorized sensitive data like passwords or session information.

Exploitation

The attackers could exploit this vulnerability in the following ways.

- Man-In-Middle-Attack: Due to weak encryption cipher mechanism the attacker can intercept encrypted communications between client and server.
- Analyzing Network Traffic: After intercepting the communications, attackers capture 32 GB or more traffic because 64 bits block cipher like 3DES tends to repeat its encryption patterns with same key.
- Session Hijacking: After creation of Collision (two blocks of plain-text producing the same cipher-text), the attacker can analyze the repeated cipher-text patterns and conclude information about the original plain-text even without decryption the data directly. This process can expose sensitive data like session cookies, authentication tokens and other confidential information.

Solutions

- SSL/TLS configurations should be preferred AES over DES.
- Remove 3DES cipher from server configuration.
- Ensure to update SSL/TLS protocols.
- Conduct security audits periodically and ensure they meet the current security standards.

CVE-2016-2118 also known as Badlock vulnerability, is a critical flaw encountered in SAMBA (open-source implementation of SMB and CIFS protocol) which enables attackers to perform Man-In-The-Middle attack and able to downgrade authentication mechanisms.

Impact on the system

- Unauthorized read/write access to the SAM (Security Account Manager) database.
- Compromise of sensitive user credentials and security policies.
- Compromises of confidentiality and integrity of system based on Samba for authentication.

Exploitation

The attackers could exploit this vulnerability in the following ways.

- Man-In-The-Middle (MITM) Attack: Attackers could exploit this vulnerability for Man-In-The-Middle attack by intercepting data between client and Samba server by using ARP (Address Resolution Protocol) spoofing or DNS (Domain Name System) poisoning to have full access to the sensitive data.
- Impersonation and Credential Theft: Attackers could use intercepted credential as legitimate users to request MS-SAMR (Security Account Manager Remote Protocol) to retrieve sensitive information like passwords, security policies or user authorizations.
- Downgrade Attack: Attacker exploits this vulnerability to compromise DCE (Distributed Computing Environment) or RPC (Remote Procedure Calls) connections which could lead to denial of service against Samba server (high CPU load) and forcing the connections to use less secure configurations like disabling encryption.
- Expanding privilege: If the Samba server is configured as an Active Directory Domain Controller, the attacker could compromise the AD objects and grant higher privileges across the network.

Solutions

- Update Samba to 4.2.11, 4.3.8, 4.4.2 or later.
- Ensure SMB signing is enabled and required for all connections.
- Configure secure authentication protocols like Kerberos and NTLMv2.
- Use additional encryption for DCE/RPC communication to prevent interception from network.
- In the case of Samba configured as a Domain Controller, implement secure policies to mitigate exploitation risks in Active Directory.
- Configure logging and monitoring tools to detect suspicious and unauthorized access attempts.

Task 3: Information Security Risk Assessment and Management

In our task 3, we performed a detailed risk assessment and management activity focused on the Marriott International Starwood 2018 data breach. We created tables that outline the inventory asset, risk register, and risk control using tools such as Common Vulnerabilities and Exposures (CVE), National Vulnerability Database (NVD), and Common Attack Pattern Enumeration and Classification (CAPEC) framework to assess vulnerabilities (Security vulnerabilities, CVEs, no date). In Table 1, we created a detailed inventory asset highlighting the name, detail, value, sensitivity, and criticality of the assets from the outcome of the vulnerabilities, threats and risk of the breach. In Table 2, we develop a comprehensive risk register table showcasing the risk identity, name, related vulnerability details, assets affected, the impact of the risk, and the level of the risk based on the impact or threat. Finally, we propose a risk control plan in Table 3 expounding on risk identity, the control strategy to be used incorporating technical control, application control, administrative control, and appropriate implementation aligning with the National Institute of Standards and Technology (NIST) cybersecurity framework.

3.1 Inventory of Assets

	Cyber Asset Name	Asset Category	Asset Details	Acceptable use of asset	Asset Value	Sensitivity	Criticality
1	Starwood Reservation Database	Software	A database contains guest booking records.	Used to store and process customer reservations data.	High	Restricted	Essential
2	Web Servers	Hardware/ Software	Physical and virtual servers hosting Marriott websites	Hosting an online platform for booking reservations.	High	Restricted	Essential
3	Data Encryption Keys	Software	It secures data in transit and at rest.	Protecting sensitive Customer data.	High	Restricted	Essential
4	Customer Web portal	Software	Front end interface for online reservations.	Customer processing	Medium	Restricted	Required
5	Point of sale system	Hardware	Handles financial transactions	Payment processing	High	Restricted	Required
6	Internal Network	Hardware	Backbone for organization's IT systems	Internal Communication	High	Restricted	Essential
7	Backup storage system	Hardware	Archives data for disaster recovery	Data recovery	High	Restricted	Required
8	Employees Devices	Hardware	Workstation and laptops for employees	Given to Marriott's employees	Medium	Restricted	Required
9	Firewall Systems	Software/ Hardware	Filters network traffics	preventing unauthorized access by giving access to only authorized employees.	High	Restricted	Essential
10	Mobile Application	Software	Marriott mobile app currently as Marriott Bonvoy	Customers interact with applications to make reservations and get rewarded loyalty points.	Medium	Restricted	Essential

Table 1 Inventory of Assets

3.2 Risk Register

Risk ID	Risk Name	Related Vulnerabilities	Threats	Affected Assets	Impact	Risk Level (Level,
R1	Database Exploitation	<p>1.CVE-2021-44228 Base Score: 10.0 Impact: High Access Complexity: Low Authentication: None Type: Remote Code Execution Level: High</p> <p>2. CVE-2021-34527 Base Score: 8.8 Impact: High Access Complexity: Medium, Authentication: None Type: Privilege Escalation Level: High</p>	<p>Exploitation via Log4j Vulnerability Level: High</p> <p>Print Spooler service improperly performs privileged file operations Level: High</p>	Starwood Reservation Database	Compromise of sensitive customer booking records	Vulnerability Level: High Threat Level: High Impact Level: High
R2	Data Breach through Web Servers	<p>1.CVE-2020-14882 Base Score: 9.8 Impact: High Access Complexity: Low Authentication: None Type: Path Traversal Level: High</p> <p>2. CVE-2021-21972 Base Score: 9.8 Impact: High Access Complexity: Low Authentication: None Type: Remote Code Execution Level: High</p>	<p>Remote Code Execution Level: High</p> <p>Exploitation via Unauthenticated Level: High</p>	Web Servers	Exposure of customer and business sensitive data	Vulnerability Level: High Threat Level: High Impact Level: High
R3	Key Exposure Risk	<p>1. CVE-2022-0778 Base Score: 7.5 Impact: High Access Complexity: Medium Authentication: None Type: Cryptography Vulnerability Level: High</p> <p>2.CVE-2020-13777 Base Score: 7.4 Impact: High Access Complexity: Medium Authentication: None Type: Cryptography Vulnerability Level: High</p>	<p>Exploitation of OpenSSL Flaws Level: High</p> <p>Weak Key Generation Level: High</p>	Data Encryption Keys	Exposure or misuse of encryption keys jeopardizing data	Vulnerability Level: High Threat Level: High Impact Level: High
R4	Network Exploitation	<p>1. CVE-2020-1472 Base Score: 10.0 Impact: High Access Complexity: Low Authentication: None Type: Privilege Escalation Level: High</p> <p>2. CVE-2021-26855 Base Score: 9.8 Impact: High</p>	Exploitation of Zero Logon Level: High	Internal Network	Disruption of communication with potential data ex-filtration	Vulnerability Level: High Threat Level: High Impact Level: High

		Access Complexity: Low Authentication: None Type: Server-Side Request Forgery Level: High	Proxy Shell Exploit Level: High			
R5	Point-of-Sale System Compromise	1. CVE-2021-36934 Base Score: 7.8 Impact: High Access Complexity: Medium Authentication: None Type: Privilege Escalation Level: High 2. CVE-2021-34527 Base Score: 8.8 Impact: High Access Complexity: Medium Authentication: None Type: RemoteCode Execution Level: High	Local Privilege Escalation via Vulnerable ACLs Level: High Print spooler remote code vulnerability Level: High	Point of Sale System	Financial losses, reputation damage	Vulnerability Level: High Threat Level: High Impact Level: High
R6	Firewall Breach	1. CVE-2022-40684 Base Score: 9.8 Impact: High Access Complexity: Low Authentication: None Type: Authentication Bypass Level: High 2. CVE-2021-27860 Base Score: 9.8 Impact: Medium Access Complexity: Medium Authentication: None Type: Privilege Escalation Level: High	Exploitation of Fortinet Firewalls Level: High Unauthorized Command Execution Level: High	Firewall Systems	Unauthorized access, risk of lateral movement	Vulnerability Level: High Threat Level: High Impact Level: High
R7	Mobile Application Vulnerabilities	1. CVE-2020-27223 Base Score: 5.3 Impact: Medium Access Complexity: Medium Authentication: None Type: Insecure API Endpoints Level: Medium 2. CVE-2021-31986 Base Score: 6.8 Impact: Medium Access Complexity: Medium Authentication: None Type: Data Exposure Level: Medium	Application Programming Interface (API) Exploitation Level: Medium Data Theft through Insecure Configuration Level: Medium	Mobile Application	Exposure of customer data	Vulnerability Level: Medium Threat Level: Medium Impact Level: Medium

Table 2 Risk Register

3.3 Risk control

RISK ID	Risk Control Strategy	General Controls and Functions	Application Controls and Functions	Administrative Controls and Functions	Duration	NIST CSF Reference (Category/Sub-category)
R1	Reduce	Implement robust encryption for database fields containing sensitive information	Enforce role-based access controls (RBAC) on the database application to limit access to sensitive records.	Carry out regular security employees training for staff handling database access. Provide updates to response plans be able to avoid database exploitation Scenarios.	3 months	Category: Protect Respond Subcategory: PR.DS-1 PR.DS-2 PR.AC-4 PR.AT-2 RS.IM-2
R2	Reduce	Harden web servers by regularly applying patches and disabling unused services.	Use Web Application Firewalls (WAF) to filter malicious traffic and implement monitoring for unusual traffic patterns.	Maintain strict change control processes and audits for deployed web server configurations.	6 months	Category: Protect, Detect Subcategory: PR.PT-3 PR.PT-4 DE.AE-2 PR. IP-3
R3	Avoid	Use hardware security modules (HSMs) for encryption key storage and processing.	Implement multi-factor authentication (MFA) for key management operation	Limit access to encryption key environments to only essential personnel. Review and rotate keys periodically	4months	Category: Protect Subcategory: PR.DS-6 PR.AC-7 PR.AC-4 PR.DS-5
R4	Reduce	Employ network segmentation to isolate critical systems and restrict lateral movement.	Deploy intrusion detection systems (IDS) and Intrusion prevention systems (IPS) to monitor network activity for ZeroLogon or ProxyShell exploit attempts.	Provide incident response training focused on network-based vulnerabilities. Establish escalation paths for critical network-related breaches.	6 months	Category: Protect, Detect Respond Subcategory: PR.PT-3 DE.CM-1 PR.PT-1 PR.AT-2 RS.RP-1 RS.CO-2
R5	Reduce	Regularly update point-of-sale systems with patches; disable default accounts and unnecessary services.	Implement application whitelisting to prevent unauthorized software installation on PoS systems.	Perform regular vulnerability assessments of Point of Sale (PoS) system. Establish audit trails for all financial transactions to trace suspicious activity.	3 months	Category: Protect Identify Detect Subcategory: PR.MA-1 PR.PT-3 ID.RA-1 DE.CM-8 PR.PT-1 DE.CM-3

R6	Reduce	Enable strict firewall rules and policies to block unauthorized access; implement centralized logging for all firewall activities.	Use virtual private network (VPN) solutions to limit direct access to network resources and ensure encrypted traffic.	Conduct regular reviews of firewall rule sets and ensure staff are trained in managing firewall configurations securely.	5 months	Category: Protect, Detect Subcategory: PR.AC-3 DE.CM-1 DE.CM-2 PR.AC-3 PR.DS-2 PR.MA-1 PR.AT-2
R7	Accept	Document risks associated with API endpoints and ensured robust monitoring for API activity; assess cost-effectiveness of endpoint vulnerability reduction measures.	Apply API rate limiting and implement OAuth-based authentication to improve API security.	Establish accountability and regular reviews of mobile app security policies; provide staff with secure app development training.	6 months	Category: Identify, Protect, Detect Subcategory: ID.RA-4 DE.CM-1 DE.CM-7 ID.RM-2

Table 3 Risk Controls

Task 4: Incident Response

4.1 Preparation

4.1.1 Purpose:

The Incident response plan focuses on establish a detailed and well-defined solution towards identifying, analyzing, managing and solving to Marriott International Starwood data breach 2018 incident. The incident response plan aims to minimize impact of the breach, protect sensitive data, reduce recovery time and create a better plan towards preventing future incidents from occurring.

The main objective of the Incident plan includes.

- Limiting damage caused in Marriott International data and system
- Effectively identifying, assessing, and manage security incidents
- Ensure a coordinated, timely and effective response plan
- Improve security posture and prevent occurrence of similar incidents
- Compliance with GDPR regulations and standards should be observed.
- Documenting what needs to be done by the team to restore the system back to normal operations.

4.1.2 Scope:

scope of the incident response plan includes all Marriott International's critical systems, networks, and databases that handle sensitive customer information, including:

- Customer reservation systems.
- Hotel management systems.
- Centralized data repositories containing guest personal and payment information.

- IT infrastructure such as servers, cloud services, and communication networks.

This plan will focus on Marriott's International global operations covering its hotels, subsidiaries and third-party service providers involved in the handling of their customers' sensitive data.

4.1.3 CSIRT Team

4.1.3.1 CSIRT Type

It will be of a centralized type that is dedicated to handling all incidents across the organization from a central location allowing smooth business operations.

4.1.3.2 CSIRT Member Type

The CSIRT will consist of a diverse group of experts from different domains of IT members, Security, communication, and legal.

4.1.3.3 Skills and Abilities

They will have great skills set to be able to keep the organization running and away from future attacks, as they will be well trained and equipped with great abilities to anticipate it.

4.1.3.4 Assign Roles and Responsibilities

The response team will be allocated different roles that suite their specialized skills to allow them focus on carrying out their allocated tasks effectively.

This team will consist of the following members:

1. **The incident response manager** who will be responsible in overseeing the general incident response plan and leading the team on cybersecurity incidents to detect, contain and recover the organizations system swiftly.
2. **Security analyst** who be responsible in monitoring systems to identify threats then analyze the incident and help in mitigating the security breach. Then investigate if any vulnerabilities are available and if they are he creates security tools to better the organizations security.
3. **IT administrator** will play a pivoted role in supporting the technical IT infrastructure when conducting an incident response plan and general cybersecurity operations while ensuring all the networks and tools required are operational and secure.
4. **IT support** team will be performing system recovery and containment measures to help the general process.
5. **Legal and compliance officer** will guide the organization response towards the incident to comply with the applicable laws and regulations based on industry standards.
6. **The Communication officer** will manage both the internal and external communication between stakeholders, clients, and press to maintain the organizations reputation throughout the incident response phase.
7. **The human resource manager** will manage employees related issues and assist affected staff on how to move forward and follow up with training and awareness on the incident.

4.2 Detection and Analysis

Detection and analysis will involve identifying potential security incidents or anomalies and examining them to determine their cause, impact, and scope. This process typically includes monitoring, alerting, and investigating data to understand threats and mitigate risks effectively.

4.2.1 Detection Strategies to be used:

- Deploy Security Information and Event Management (SIEM) systems to gather and analyze logs from multiple sources, enabling the detection of potential security incidents.
- Perform regular vulnerability assessments and penetration testing to identify and address weaknesses in the organization's infrastructure.
- Establish a robust threat intelligence program or utilize machine learning-based systems to stay informed about emerging attack vectors and indicators of compromise
- Continuously monitor hotel systems and terminals to detect unusual activities or unauthorized access attempts.
- Ensure customers' endpoints are regularly scanned for anomalies and unauthorized access to protect their data and maintain security.
- Implement Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor network traffic and identify suspicious activities in real-time.

4.2.2 Attack Vectors to Consider

- phishing attacks targets employees or customers through deceptive emails that appear to be from legitimate sources, with the intent to steal sensitive personal or financial information.
- Attackers exploited vulnerabilities in software systems, taking advantage of unpatched security flaws to gain unauthorized access, compromise data, or disrupt organizational operations.
- Insider threats arise when employees or contractors misuse their access to company resources, intentionally or unintentionally causing harm, stealing data, or sabotaging the organization.
- Social engineering techniques manipulate employees into revealing confidential information by impersonating trusted figures within or outside the organization.
- Advanced Persistent Threats (APTs) involving sophisticated attackers who infiltrate the organization's network, remaining undetected for extended periods while stealing valuable data and spying on the system.

4.2.3 Data Categories/Types of Data to Collect:

- Personally Identifiable Information (PII), such as email addresses and phone numbers can be collected for user authentication but must be safeguarded to prevent breaches.
- User activity logs track login times and accessed resources, helping to monitor usage and detect unauthorized access.
- Session logs capture user actions and session duration, aiding in troubleshooting and identifying security risks.
- Network traffic data monitors data flow to detect threats and ensure network security.
- System and application logs document events and usage, assisting in issuing diagnosis and maintaining system security.

4.2.4 Source of the Data:

- Tracking and analyzing security incident incidents using monitoring tools.
- Recording network and security logs to detect threats.
- Internal Systems from Marriott internal network and servers
- Forensic analysis of Starwood systems.
- External threat intelligence sources on similar attacks
- Third party vendors handling payment and reservation systems

4.2.5 Prioritization of incidents

Organizations should ensure the prioritize cybersecurity measures like strong access restrictions, performing regular system updates and patches, encrypting sensitive data while conducting security audits regularly. They should also ensure their employees are offered proper training with a clear knowledge of security incidents occurring. Prioritization of incidents should be conducted based on severity, impact and score of the incident. Prioritization should be done based on:

Critical Incidents: Breaches involving substantial volumes of client data with financial and personally identifying information.

High Priority Incidents: This includes attacks that take advantage of vulnerabilities available in systems.

Low Priority Incidents: These are incidents that occur but lack evidence of data compromise as they leave minor impacts.

4.3 Containment, Eradication and Recovery

4.3.1 Containment Measure and Description

After the occurrence of the data breach Marriott International should isolated the affected systems and networks to prevent the spread of the vulnerability. This should be conducted by disconnecting all compromised devices from the network and conducting network segmentation to ensure the attack does not continue. Accounts that could have been compromised should be disable and reset of users' credentials conducted to eliminate unauthorized access privileges.

To effectively carry out containment measures for the Marriott International Starwood data breach of 2018, the CSIRT team must take a coordinated approach involving each member's expertise. The incident response manager would oversee the containment strategy, ensuring that all team members are aligned and implementing rapid actions to isolate the breach and prevent further data ex-filtration. The security analyst would begin by analyzing logs and system behavior to identify the point of compromise, determining the scope of the attack, and using detection tools to detect any residual threats. The IT administrator would then implement technical controls, such as disabling compromised accounts, isolating affected systems, and blocking external communications channels, while also ensuring that the organization's networks remain secure and operational. The IT support team would focus on recovering critical systems and restoring services with secure backups, ensuring that compromised systems are not brought back online without addressing the underlying vulnerabilities. The legal and compliance officer would ensure that all containment actions are compliant with data protection laws, particularly in relation to the breach of personal data, and would help prepare any necessary regulatory reports. The communication officer would work to keep internal and external stakeholders informed, managing sensitive communications regarding the breach and maintaining the company's reputation. Lastly, the human resource manager would assist affected employees, guiding them on how to proceed in case of personal data exposure, and ensuring that staff are educated on the incident's lessons through follow-up training and awareness sessions. Together, this comprehensive approach would help minimize the damage and prevent the attack from spreading further within Marriott's systems.

4.3.2 Eradication Measure and Description

To eradicate the incident, the team need to identify where the weakness was and how it started. To achieve results a detailed analysis need to be conducted to uncover underlying faults to eliminate malicious software, backdoors, and unauthorized scripts. Implement patches, revoke unnecessary access privileges, and conduct security scans to mitigate risks of recurrence.

The eradication phase follows the containment phase in an incident response plan and focuses on removing the root cause of the breach to restore security and operational integrity. During the eradication of the Marriott Starwood breach, the Forensic Experts used advanced digital forensic tools to identify and remove malicious software, scripts, and backdoors that facilitated unauthorized access. IT Administrators rebuilt compromised systems from clean backups, ensuring that no residual malicious code remained, and operational functionality was restored.

Additionally, Security Analysts conducted access control reviews, auditing user privileges and revoking permissions for unused or elevated accounts to minimize future exploitation risks. Regular vulnerability scans and penetration testing were also carried out under the purview of Vulnerability Management, led by Security Analysts and supported by IT Administrators, to identify and patch all exploited vulnerabilities.

The objective of the eradication phase is ensuring the threat is removed completely and stronger security measures are in place restoring systems to their secure and original state, preventing future incidents.

4.3.3 Recover Measure and Description

To be able to maintain normal operations all affected guest reservation systems needs to be backed up safely after rigorous testing and implementation of enhanced security controls to prevent re-infection. Providing timely communication to affected users and offering support to help safeguard their personal information.

The recovery phase focuses on reestablishing normal operations while ensuring long-term security and rebuilding customer trust. In this phase, systems compromised during the Marriott Starwood breach were restored from clean and securely stored backups, ensuring critical systems such as reservation databases and web servers were fully functional. These restored systems underwent extensive testing and validation to verify their performance, integrity, and security, ensuring that no residual vulnerabilities or threats remained.

Additionally, Marriott prioritized customer communication by notifying their clients about the incident while monitoring their credit transactions to mitigate the risk of identity theft. To strengthen resilience, updated incident response policies were introduced to oversee the recurrence of similar incident. Finally, compliance reviews were conducted in close collaboration with regulators to confirm adherence to regulations such as GDPR to ensuring legal and regulatory requirements were met. This comprehensive recovery effort allowed Marriott to restore operations securely and regain customer confidence.

Self-Reflection

ROP PHYLLIS JEBICHII

2707571

1. My contribution to the coursework has enabled me to gain profound knowledge and understanding into cybersecurity incident management. Throughout the coursework my partner and I worked collaboratively to ensure we got an insight into each Task, applying knowledge gathered from the deep research conducted.

In Task one, I investigated the incident details and Cyber Threat Intelligence Analysis which gave me an understanding of how the Marriott International Starwood data breach 2018 occurred and how millions of customers were affected. The Cyber Threat Intelligence Analysis deepened my understanding into leveraging threat intelligence sources to anticipate and reduce potential risks.

In Task two, we conducted an automated vulnerability scan and analysis using tools like Nmap and Nessus on a virtual machine called Metasploitable. We were able to identify vulnerabilities and analyse CVEs based on their severity using CVSS score gathering knowledge on how to identify vulnerabilities.

In task three, we used the recommended resources like Common Vulnerabilities and Exposures (CVE), NVD, and CAPEC to create tables of Inventory asset, Risk register and Risk controls.

Finally, we contributed to developing a clear response plan in Task 4 focusing on preparation, detection, containment, eradication, and recovery of our case study highlighting the importance of a structured responses, teamwork, and proactive measures in an organization.

2. The Marriott International Starwood 2018 incident highlights the critical vulnerabilities faced by organizations when managing customers sensitive data across complex IT infrastructures. The breach was caused by Marriott's poor security practices during the integration process as the Starwood systems had already been compromised before its acquisition in 2016, allowing an inherited vulnerability. The inadequate security practices caused a delay in detecting the unusual activities ongoing in the Starwood reservation database compromising approximately 500 million customer records. The failure to have advanced monitoring tool, updated security protocols and encryption across all sensitive data created a great reputation damage for Marriott international as attackers were using Remote access Trojans and Mimikatz to exploit them. The breach further incurred a great financial loss as a fine of £18.4 million was imposed by UK's Information Commissioner's Office (ICO).

This incident would have been avoided by Marriott International if they had performed a proper integration of Starwood into their system after acquisition and ensured proper multi-factor authentication process on customer sensitive records.

To tackle cyber-attacks trends in the future, organizations need to adopt a proactive and well-defined security approaches into operations to safeguard their client's data. These approaches include adapting to Zero trust architectures to restrict access to only authorized persons. Regularly updating and patching software and systems using advanced tools like AI-powered anomaly detection to deploy Security Information Event management (SIEM) can help identify and neutralize threats before they escalate. Cyber resilience requires consistent employee training on recognizing phishing attempts and social engineering tactics, as human error remains a significant vulnerability. Additionally, organizations should foster robust vendor management practices and conduct third-party risk assessments to safeguard supply

chain security. These measures with enhanced encryption and backup policies combined with regulation standards will help mitigate the impact of future cyber-attacks.

SAURAV GURUNG

U2773653

1. During this coursework, I gained knowledge regarding real-world challenges faced by organizations due to different cyber threats and the fighting tactic against these threats for safeguarding sensitive information from any unauthorized access.

In Task1, I learned the importance of incident analysis to identify the root cause and weakness, such as outdated infrastructure, weak access controls and inadequate monitoring systems could allow attackers to gain sensitive information and maintain undetectable for long period of time.

In Task2, we used vulnerability assessment tools like Nmap and Nessus. We were provided with a virtual machine called Metasploitable where my partner and I collaborated to scan and find out all the vulnerabilities. We used Nessus to identify the potential vulnerabilities in the system which provided us with the scan report mentioning proper CVE with security levels and CVSS score.

In Task3, we gained security understanding of conducting information security risk assessment and management on any organization by creating inventory of assets, risk register and risk controls.

Finally, Task4 taught us the incident response process which helped us to understand the structured approach required to handle any security breaches. My partner and I explored the attributes like preparation, detection, analysis, containment, eradication and recovery to create proper Incident Response Plan.

2. The Marriott International data breach occurred mainly due to serious security weakness in the Starwood database system that Marriott acquired. The outdated infrastructure, poor access controls and lack of proper network segmentation led to compromise the sensitive information of customers. The attackers remain unnoticeable from 2014 to 2018 which shows lack of proper monitory tools and security patches not applied regularly. The attackers used Remote Access Trojans and Mimikatz tools for attack which significantly consequences loss of trust, financial penalties and regulatory review such as fines under GDPR.

The case study on Metasploitable VM scanning further enhanced my technical understanding of how vulnerabilities can be exploited. By using Nmap it helped me to find out the open services running like Telnet, unknown ports opened could be vulnerable if not configured securely. Nessus helped me to identify vulnerabilities classified into high, medium and low severity. For example, the CVE-2016-2183 (SWEET32) vulnerability demonstrated how weak encryption could allow attackers to recover sensitive information. Similarly, CVE-2016-2117 (Badlock) showed how authentication weakness in Samba could lead to privilege escalation and compromise sensitive data.

To mitigate from such future cyber-attacks trends, organizations must focus on proactive security measures like regular Vulnerability Assessment and Penetration Testing (VAPT), implementing multi-factor authentication, industry practice encryption mechanisms and role-based access controls. Tools like SIEM and IDS should be deployed to monitor real time activity on the network.

Day to day social engineering attacks is evolving with more advanced tactics so the employee should be well trained. There should be proper security audits and integration checks to identify vulnerabilities on legacy systems. All the employees or system should be zero-trusted and should update response plans continuously for preparing organizations with evolving threats.

Presentation Slides



Figure 4 Slide 1

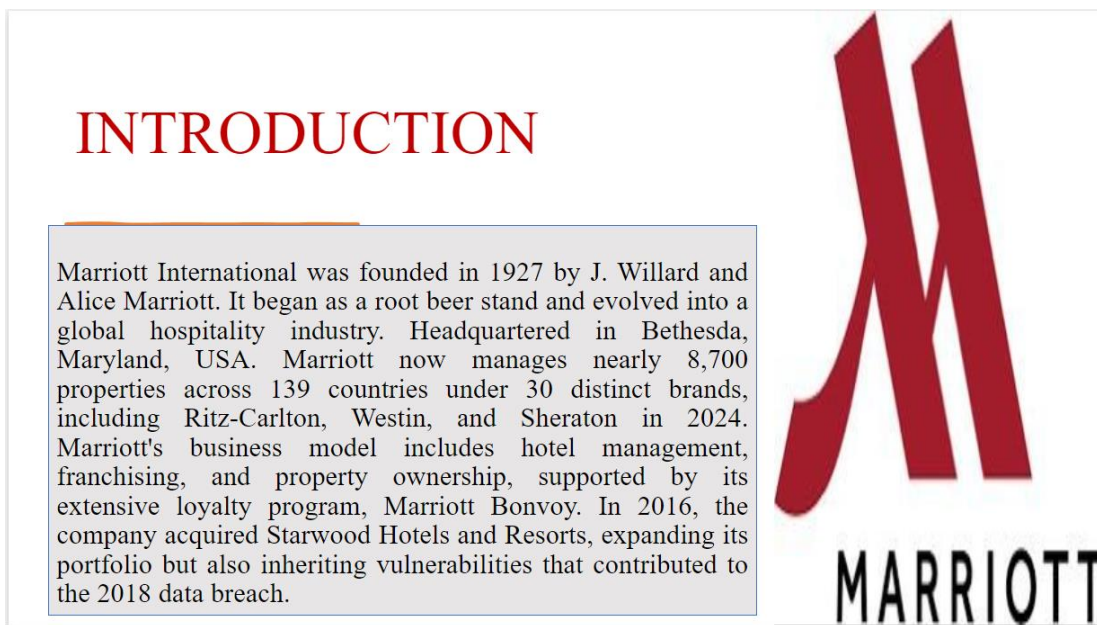


Figure 5 Slide 2



INCIDENT DETAILS

Unusual activity was flagged: 8th September 2018

Date of Discovery: 19th November 2018

Public Disclosure: 30th November 2018.

Breach Duration: 2014 - 2018.

Type of Incident: Data breach via unauthorized access to Starwood guest reservation database.

Figure 6 Slide 3

SOURCES USED FOR THE RESEARCH

- Use of industry reports, case studies and cybersecurity framework like NIST and CVE.
- Gathered information from the sources like wired.com and CSO online, ICO, ResearchGate, BBC news, and more.
- Official reports from Marriott and regulatory bodies.

Figure 7 Slide 4

CAUSE OF DATA BREACH

- In 2014, the attacker first might have identified the vulnerability like poor input validation or miss configuration permission which allowed them to upload the web shell on web server.
- The attacker penetrated the Starwood network using a web shell as a backdoor.
- They used Remote Access Trojan (RAT) and Mimikatz.
- The attackers successfully bypassed Starwood's access control which indicates weakness in the network's authentication and authorization mechanism.
- The organization lacked proper access control mechanism, lack of multi-factor authentication system for critical user, and human error for not maintaining high security which made attack successful to be undetectable for long period of time.

Figure 8 Slide 5

The screenshot displays the Marriott Bonvoy website interface. On the left, a large red text overlay reads "Sensitive Customer's Data Breached". The main content area shows a registration form for a Marriott Bonvoy account. The form includes fields for First Name, Last Name, Country/Region (set to USA), Zip/Postal Code, Email, Password, and Date of Birth. A "Sign Up" button is visible. To the right of the form, a "Personal Info" sidebar contains fields for Country/Region, Zip/Postal Code, Address Line 1, Address Line 2, City, State/Province, Email, Re-enter Email, Country Code, Mobile Phone Number, and Home Phone Number. A "Book Now" button is also present. At the bottom, a "Member Number" field displays "465306862" and a "Passport Number" field is labeled.

Figure 9 Slide 6

RECOMMENDATIONS FOR FUTURE ATTACKS

- Adopt-zero trust architecture
- Implement advanced monitoring tool
- Regular employee training and awareness
- Enhance data encryption and backup policies

Figure 10 Slide 7



LESSONS LEARNT AND FUTURE DIRECTIONS

- Emphasize the seamless integration of cybersecurity measures when merging systems to avoid inherited vulnerabilities.
- Prioritize the security of outdated systems by upgrading, patching, or replacing them to prevent exploitation.
- Ensure that all systems are updated with the latest security patches to address known vulnerabilities.
- Implement and enforce robust access control measures to limit unauthorized access to sensitive data.

Figure 11 Slide 8

References

- Amanulla, A. and Niyaz, S. (2024) 'Marriot Data Breach: A Case Study Analysis', *Information Technology Security and Risk Management: Inductive Cases for Information Security*, pp. 241–245. Available at: <https://doi.org/10.1201/9781003264415-35/MARRIOT-DATA-BREACH-AREEB-AMANULLA-SAADIK-NIYAZ>
- Denuwan, R. (no date) 'Marriott International Data Breach'. Available at: <https://www.researchgate.net/publication/372524901> (Accessed: 18 December 2024).
- John Breeden II (2022) *What is Nmap and why do you need it on your network?* | *Network World*. Available at: <https://www.networkworld.com/article/966196/what-is-nmap-why-you-need-this-network-mapper.html> (Accessed: 19 December 2024).
- Josh, F. (2020) *Marriott data breach FAQ: How did it happen and what was the impact?* | *CSO Online*. Available at: <https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html> (Accessed: 19 December 2024).
- Marriott Announces Starwood Guest Reservation Database Security Incident* (no date). Available at: <https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident> (Accessed: 18 December 2024).
- 'Marriott International Inc, Penalty Notice - 30 October 2020' (no date).
- Security vulnerabilities, CVEs*, (no date). Available at: <https://www.cvedetails.com/vulnerability-list> (Accessed: 18 December 2024).
- Alshorman, R. and Al-Ofeishat, H.A. (no date) 'Build a Secure Network Using Segmentation and Micro-segmentation Techniques', *International Journal of Computing and Digital Systems*, 16(1), pp. 2210–142. Available at: <https://doi.org/10.12785/ijcds/1601111>.
- Amanulla, A. and Niyaz, S. (2024) 'Marriot Data Breach: A Case Study Analysis', *Information Technology Security and Risk Management: Inductive Cases for Information Security*, pp. 241–245. Available at: <https://doi.org/10.1201/9781003264415-35/MARRIOT-DATA-BREACH-AREEB-AMANULLA-SAADIK-NIYAZ>.
- CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™)* (no date c). Available at: <https://capec.mitre.org/> (Accessed: 18 December 2024).
- Cyber Case Study: Marriott Data Breach - CoverLink Insurance - Ohio Insurance Agency* (no date a). Available at: <https://coverlink.com/case-study/marriott-data-breach/> (Accessed: 18 December 2024).
- Cyber Case Study: Marriott Data Breach - CoverLink Insurance - Ohio Insurance Agency* (no date b). Available at: <https://coverlink.com/case-study/marriott-data-breach/> (Accessed: 18 December 2024).
- Cyber Case Study: Marriott Data Breach - CoverLink Insurance - Ohio Insurance Agency* (no date c). Available at: <https://coverlink.com/case-study/marriott-data-breach/> (Accessed: 18 December 2024).
- Cybersecurity News, Insights and Analysis | Security Week* (no date). Available at: <https://www.securityweek.com/> (Accessed: 18 December 2024).
- Denuwan, R. (2023 a) 'Marriott International Data Breach'. Available at: <https://www.researchgate.net/publication/372524901> (Accessed: 18 December 2024).
- Josh, F. (2020) *Marriott data breach FAQ: How did it happen and what was the impact?* | *CSO Online*. Available at: <https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html> (Accessed: 19 December 2024).
- Marriot Data Breach | 35 | A Case Study Analysis | Areeb Amanulla, Saa* (no date). Available at: <https://www.taylorfrancis.com/chapters/edit/10.1201/9781003264415-35/marriot-data-breach-areeb-amanulla-saadik-niyaz> (Accessed: 18 December 2024).
- Marriott Announces Starwood Guest Reservation Database Security Incident* (no date a). Available at: <https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident> (Accessed: 18 December 2024).
- Marriott Announces Starwood Guest Reservation Database Security Incident* (no date b). Available at: <https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident> (Accessed: 18 December 2024).
- Marriott Announces Starwood Guest Reservation Database Security Incident* (no date c). Available at: <https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident> (Accessed: 18 December 2024).
- Marriott breach potentially exposed data of 500m guests* (no date). Available at: <https://www.ft.com/content/1a4a5dea-f492-11e8-9623-d7f9881e729f> (Accessed: 18 December 2024).

Marriott data breach FAQ: How did it happen and what was the impact? | CSO Online (no date a). Available at: <https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html> (Accessed: 18 December 2024).

Marriott ends 2018 ahead despite data breach, strikes (no date). Available at: <https://vtechworks.lib.vt.edu/items/c17eaccb-8ea0-45e3-ab35-4a8cb811ab4f> (Accessed: 18 December 2024).

Marriott Got Hacked. Yes, Again | WIRED (no date). Available at: <https://www.wired.com/story/marriott-hacked-yes-again-2020/> (Accessed: 18 December 2024).

Marriott International Update on Conclusion of UK ICO Investigation into Starwood Database Security Incident (no date). Available at: <https://news.Marriott.com/news/2020/10/30/marriott-international-update-on-conclusion-of-uk-ico-investigation-into-starwood-database-security-incident> (Accessed: 18 December 2024).

Marriott News Center (no date c). Available at: <https://news.marriott.com/> (Accessed: 18 December 2024).

Mest, E. (2019) 'Marriott ends 2018 ahead despite data breach, strikes'. Available at: <http://hdl.handle.net/10919/88403> (Accessed: 18 December 2024).

NVD - Search and Statistics (no date). Available at: <https://nvd.nist.gov/vuln/search> (Accessed: 18 December 2024).

(PDF) *Marriott International Data Breach* (no date a). Available at: https://www.researchgate.net/publication/372524901_Marriott_International_Data_Breach (Accessed: 19 December 2024).

(PDF) *Marriott International Data Breach* (no date b). Available at: https://www.researchgate.net/publication/372524901_Marriott_International_Data_Breach (Accessed: 18 December 2024).

Stefaniuk, T. (2020) 'ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES 1832 TRAINING IN SHAPING EMPLOYEE INFORMATION SECURITY AWARENESS', 7(3), pp. 1832–1846. Available at: [https://doi.org/10.9770/jesi.2020.7.3\(26\)](https://doi.org/10.9770/jesi.2020.7.3(26)).

The data breach that cost Marriott £18.4 million - what went wrong? | Data Protection Network (no date a). Available at: <https://dpnetwork.org.uk/data-breach-costs-marriott-18-million/> (Accessed: 18 December 2024).

Vigenesh, M. et al. (2024) 'Applying Machine Learning to Strengthening Cyber Security', 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1–6. Available at: <https://doi.org/10.1109/ICCCNT61001.2024.10723995>.