Visa Technology Traineeship Program
Ngee Ann Polytechnic

Capstone Project

[4GUYSCOFFEE]

Final Report

Networking & IT Infrastructure|

Windows & Linux Server Administration|

Cloud Systems Administration|

Cybersecurity Fundamentals|

Ethical Hacking and Pentesting|

Cybersecurity Operations|

Cyber Forensics Investigation|

Cybersecurity Risk and Compliance|

Contents

Executive Summary 3
Background 4
1. Networking & IT Infrastructure 8
2. Windows & Linux Server Administration 30
3. Secure Cloud Environment 43
4. Cybersecurity Fundamentals 51
5. Ethical Hacking and Pentesting 58
6. Cybersecurity Operations 69
7. Cybersecurity Forensics 90
8. Cybersecurity GRC 100
Capstone Conclusion 157
Team Member Contributions 158
References 159

Executive Summary

4GuysCoffee, a Singapore-based small and medium enterprise, is a premier destination for exceptional coffee experiences. Operating exclusively within the dynamic city-state of Singapore, we curate an exquisite selection of premium coffee beans sourced from diverse countries, ensuring a rich and high-quality offering. Our local facility in Singapore meticulously roasts and processes these beans, packaging them for sale and use in our six cafes spread across the city-state.

This detailed report navigates through the intricacies of our network infrastructure, which was strategically designed at our Singapore headquarters and empowered by cutting-edge tools from Cisco. Our deployment encompasses advanced configurations of switches, routers, and access points, ensuring impeccable connectivity and performance. To elevate organisational efficiency, we have implemented a sophisticated network design, utilising subnets and Virtual Local Area Networks (VLANs) to segregate departments within our headquarters. This fortifies network security and streamlines data traffic, optimising overall network management.

Embracing the cloud for scalability and adaptability, we have established a robust web server through an Elastic Compute Cloud (EC2) instance on Amazon Web Services (AWS). This cloud-centric approach guarantees reliable web hosting capabilities. Our identity management system revolves around Windows Active Directory at our Singapore headquarters, providing a centralised and secure means of user authentication and authorisation. Concurrently, an on-premise local file server facilitates seamless collaboration among our internal teams. We have incorporated an AWS file server to expand our data storage capabilities, exploring diverse storage solutions like Amazon S3 for off-site backup, enhanced data redundancy, and accessibility.

To meet the operational requirements of our cafe managers, we have implemented a dedicated PC setup in our 4GuysCoffee cafes. Through a secure Virtual Private Network (VPN) connection, branch managers can access the file server at the headquarters, facilitating swift retrieval of Point of Sale (POS) materials and critical information. This strategic integration of networking tools, cloud services, and on-premise solutions underscores 4GuysCoffee's commitment to establishing a resilient and efficient IT infrastructure aligned with our organisational goals. It is tailored to support seamless operations within Singapore's dynamic and thriving coffee scene.

Background

4GuysCoffee, a thriving small and medium enterprise headquartered in Singapore, has made a significant mark in the competitive and dynamic coffee industry. Our commitment to delivering exceptional coffee experiences is evident in our focus on using ethically sourced and sustainably grown beans, which are meticulously roasted and packaged in a local facility. This emphasis on sustainability aligns with the growing consumer demand for ethically sourced and environmentally friendly products in the global coffee market.

The company's cafes serve as more than just retail spaces; they are vibrant hubs that offer a diverse range of specialty coffees, providing customers with a unique and memorable coffee culture experience. Whether it is the aromatic blends, distinct brewing techniques, or the ambience of our cafes, 4GuysCoffee has carved a niche for itself in an industry where quality and innovation are paramount.

In addition to its physical presence, 4GuysCoffee has ventured into the digital realm by launching a global e-commerce store. This strategic move allows us to reach coffee enthusiasts worldwide, offering our signature roasted coffee beans for sale online. This expansion into e-commerce reflects the company's adaptability and recognition of evolving consumer preferences, especially when online shopping for speciality products has become increasingly popular.

- Ficticious SME Profile:
    - Name of the SME - 4GuysCoffee
    - Industry: In the dynamic coffee industry, 4GuysCoffee faces challenges such as intense competition, navigating a complex supply chain for sourcing sustainable beans, staying attuned to rapidly evolving consumer trends, and potential impacts from global economic fluctuations. However, the company is well-positioned to capitalise on promising prospects. The expanding global coffee culture, with an increasing appreciation for speciality and artisanal offerings, allows 4GuysCoffee to distinguish itself. The recent launch of our e-commerce store aligns with the rising trend of online shopping for speciality products, offering access to a broader global customer base. By maintaining a commitment to sustainability and locally sourced beans, the company aligns with the growing consumer demand for eco-friendly and socially responsible products. Moreover, opportunities for innovation in brewing techniques and flavour profiles and the cultural diversity of operating in multiple countries present avenues for growth and enhanced market appeal. Navigating these challenges while leveraging these prospects requires a strategic and adaptable approach, positioning 4GuysCoffee for continued success in the evolving global coffee landscape.

- Size and Location: Geographical distribution of HQ and branch offices
  - **Employee Breakdown:**
    Singapore: 160 pax + 1 General Manager = **161 pax**

Department	Head Count	Head of Dept	Branch Manager
Technology	3	1	-
HR	2	1	-
Customer Service	2	1	-
Sales & Marketing Ecom	9	1	-
Logistics	9	1	-
Roasting Facility	9	1	-
Cafe Staff (6 Outlets)	19 x 6 = 114	-	6

  - Geographic distribution (HQ and branch offices).

Singapore	
Cafe Outlets - Tampines: 1 - Orchard: 1 - Jewel: 1 - Jurong East: 1 - Sentosa: 1 - Paya Lebar: 1	6

  - Singapore is our headquarters, serving as the epicentre of our operations where our entire workforce is based. A dedicated team oversees the management of our global e-commerce store, which is designed to ship our exceptional coffee products worldwide. The core of our coffee production, encompassing bean roasting and packaging, will be in Singapore. To optimise the performance and responsiveness of our e-commerce page for international customers, we have strategically chosen AWS CloudFront. This content delivery network ensures efficient page loading times through its extensive network of edge locations, contributing to an enhanced online shopping experience.

    We are committed to providing an exceptional coffee experience. To execute this strategy, outlet managers oversee our cafe operations and focus on creating a unique and tailored cafe experience. This streamlined approach ensures that our workforce aligns with the specific needs of each location within Singapore.

Simultaneously, our centralised e-commerce team, headquartered in Singapore, manages our online store's global reach and efficiency (4GuysCoffee.com). By centralising our e-commerce operations in Singapore, we can effectively coordinate and optimise our online presence, providing customers worldwide with easy access to our premium coffee beans. This strategic alignment supports our commitment to delivering high-quality coffee experiences locally and globally, all from our central hub in Singapore.

- Technology Requirements:
  - The IT ecosystem accommodates diverse devices, allowing employees and external vendors to integrate their hardware and access the infrastructure remotely seamlessly. This inclusive approach fosters flexibility and accessibility.
  - The comprehensive IT infrastructure may comprise various components, including endpoints such as desktops, laptops, smartphones, servers, and diverse IoT devices. Network devices like switches, routers, gateways, and access points form the backbone of the connectivity landscape.
  - Regarding security, distinct zones such as intranets, extranets, DMZ, and VLANs are implemented to fortify the defence mechanisms. Security controls encompass a broad spectrum, including identity and access control, anti-malware solutions, application security, data loss prevention (DLP), email security, server and endpoint security, firewalls, intrusion prevention systems, security information and event management (SIEM), virtual private networks (VPN), web security, and wireless security.
  - Additionally, web applications are pivotal, featuring a corporate website and a streamlined e-commerce platform. Collectively, these components form a robust and flexible technological foundation tailored to meet the SME's specific needs and security requirements.

- Business Objectives:
  - The enhanced IT infrastructure at 4GuysCoffee is a strategic enabler aligning seamlessly with the SME's overarching business goals and objectives. By leveraging advanced networking tools from Cisco, the meticulously configured network infrastructure optimises connectivity and performance, reflecting the company's commitment to operational excellence. Implementing subnets and Virtual Local Area Networks (VLANs) within the head office underscores a dedication to enhanced security and streamlined data traffic management, supporting overall network efficiency. Embracing the cloud through an Elastic Compute Cloud (EC2) instance on Amazon Web Services (AWS) positions 4GuysCoffee for scalability and flexibility in its expanding global operations, especially with the recent launch of the e-commerce

store. Integrating Windows Active Directory for identity management and on-premise and cloud-based file servers enhances collaborative capabilities while ensuring secure user authentication and authorisation. Incorporating AWS storage solutions, including Amazon S3, expands data storage capabilities and aligns with the business objective of ensuring data redundancy and accessibility. Establishing a secure Virtual Private Network (VPN) connection for branch managers reflects the company's commitment to operational cohesion and responsiveness across diverse locations, fostering an environment conducive to efficient Point of Sale (POS) material retrieval. In essence, this strategic enhancement of IT infrastructure at 4GuysCoffee is a testament to its dedication to establishing a robust and efficient technological foundation that seamlessly supports the SME's organisational goals and operational aspirations.

1. Networking & IT Infrastructure

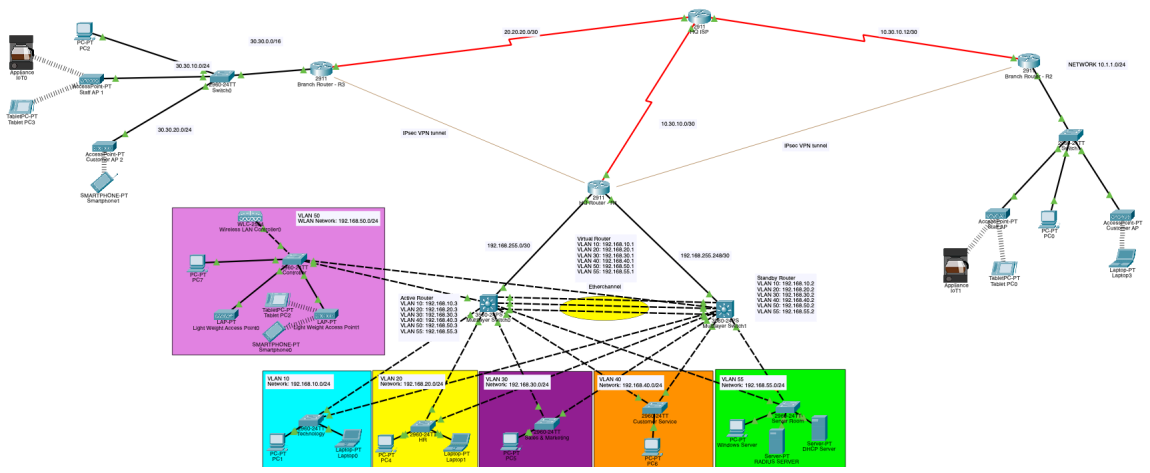
Overview

The network architecture adopts a best-in-class approach by implementing a 3-tier hierarchical design for the headquarters and a relatively simple design for the branches, widely acknowledged as an industrial best practice for creating reliable, scalable, and cost-effective networks (GeeksforGeeks, 2022). This design optimises network performance, facilitates seamless scalability to accommodate future growth, and ensures cost efficiency in network management and maintenance. The hierarchical structure provides a clear separation of functions, enhancing overall network reliability and robustness.

Distribution & Core Layer:

- The network infrastructure is designed with a robust and resilient architecture, featuring a single HQ-router complemented by two multilayer switches for efficient inter-VLAN routing and enhanced redundancy through HSRP configuration. An EtherChannel is implemented between the switches to optimise bandwidth and load balancing, significantly boosting overall network performance. The utilisation of subnets and VLANs in tandem forms a multilayer security approach, strategically addressing vulnerabilities in both Layers 2 and 3.
- To future-proof the network for business growth, subnet selection follows Cisco's addressing guide recommendations, employing VLSM while allowing space for growth /16 and /24 for the HQ and various departments, ensuring scalability. Layer 2 security is prioritised with measures like PortFast, BPDUguard, port security, and auto-trunking disabling to fortify against potential attacks.
- Routing is achieved through OSPF, chosen for its compatibility with heterogeneous networks, as opposed to EIGRP, which is limited to homogeneous networks. WLAN security is bolstered with RADIUS server authentication, providing users with unique username and password combinations for heightened access control. For secure site-to-site connections, IPSec VPNs are implemented.

Network Diagram



Network Specifications

Subnet Assignments

Location	VLAN	Subnet/Network	Department
Headquarters		192.168.0.0/16	
	10	192.168.10.0/24	Technology
	20	192.168.20.0/24	HR
	30	192.168.30.0/24	Sales & Marketing
	40	192.168.40.0/24	Customer Service
	50	192.168.50.0/24	WLAN
	55	192.168.55.0/24	Server
	99	192.168.99.0/24	Management
Branch 1		10.1.0.0/16	
	10	10.1.10.0/24	Staff
	20	10.1.20.0/24	Customers
Branch 2		30.30.0.0/16	
	10	30.30.10.0/24	Staff
	20	30.30.20.0/24	Customers

Table 2.1: Subnet address range.

MLS1-WAN	192.168.255.0/30
MLS2-WAN	192.168.255.248/30
HQ Router-ISP	10.30.10.0/30
ISP-BRANCH 1	20.20.20.0/30
ISP-BRANCH 2	10.30.10.12/30

Table 2.2: IP network addresses between the interfaces.

IP Addressing Scheme

The devices in the network are assigned the following IP Address range as defined in Table 2.3.

Device Type	Assignable IP Addresses
HQ	
Any wired device in Technology (VLAN 10)	192.168.10.4 to 192.168.10.243
Any wired device in HR (VLAN 20)	192.168.20.4 to 192.168.20.243
Any wired device in Sales(VLAN 30)	192.168.30.4 to 192.168.30.243
Any wired device in Customer Service (VLAN 40)	192.168.40.4 to 192.168.40.243
Any wirelessly connected device (VLAN 50)	192.168.50.4 to 192.168.50.243
Active Directory Windows Server (VLAN 55)	192.168.55.6
DHCP Server (VLAN 55)	192.168.55.4
RADIUS Server (VLAN 55)	192.168.55.5
JEWEL BRANCH	
Any wired or wireless device - Staff (VLAN 10)	10.1.10.2 to 10.1.10.254
Any wireless device - Customers (VLAN 20)	10.1.20.2 to 10.1.20.254
ORCHARD BRANCH	
Any wired or wireless device - Staff (VLAN 10)	30.30.10.2 to 30.30.10.254
Any wireless device - Customers (VLAN 20)	30.30.20.2 to 30.30.20.254

Table 2.3: Allotment of IPv4 addresses for different device types.

System Configurations

HQ - Switches & Routers

Basic Device Configuration (VLAN Creation for HQ switches).

Creating VLANs on switches

```
configure terminal
vlan 10
name Technology
exit
vlan 20
name HR
exit
vlan 30
name Sales
exit
vlan 40
name Cust
exit
vlan 50
name WLAN
exit
vlan 55
name Server
exit
vlan 99
name Management
exit

int range fa0/1-2
switchport mode trunk
exit

int range fa0/3-24
switchport mode access
switchport access vlan 10
exit
```

Figure 2.1: Sample configuration for VLAN creation and setting up trunk ports on HQ switches.

```
SW-Tech(config)#exit
SW-Tech#
%SYS-5-CONFIG_I: Configured from console by console

SW-Tech#
SW-Tech#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1, Gig0/2
10   Technology                        active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
20   HR                                active
30   Sales                             active
40   Cust                              active
50   WLAN                              active
55   Server                            active
99   Management                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
SW-Tech#sh ip int
SW-Tech#sh ip interface ?
  Vlan   Catalyst Vlans
  brief  Brief summary of IP status and configuration
  |      Output Modifiers
  <cr>
SW-Tech#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
FastEthernet0/4        unassigned      YES manual up                    up
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual administratively down down
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual administratively down down
FastEthernet0/21       unassigned      YES manual administratively down down

SW-Tech#
```

Top

Figure 2.2: Verification of VLANs and port allocations and shutdown of unused ports for added security.

```
int vlan 55
ip add 192.168.55.2 255.255.255.0
no shut
standby 55 priority 90
standby 55 ip 192.168.55.1
exit


Config for OSPF
router ospf 25
router-id 1.3.1.3
network 192.168.255.248 0.0.0.3 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.55.0 0.0.0.255 area 0
```

Figure 2.3: Commands for configuration of MLSs of VLAN interfaces, HSRP & OSPF.

Similar commands execute the VLANs created on the MLSs to the switches i.e:

vlan 10

name Technology

Then, the VLAN interfaces are created, and an IP address is assigned. For HSRP, we put a priority number and then allocate a standby IP address of the virtual router. Following that, we can configure OSPF routing protocol for the MLSs by advertising the adjacent networks.

```
MLS1-HQ#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   100   Active   local           192.168.10.2    192.168.10.1
Vl20        20   100   Active   local           192.168.20.2    192.168.20.1
Vl30        30   100   Active   local           192.168.30.2    192.168.30.1
Vl40        40   100   Active   local           192.168.40.2    192.168.40.1
Vl50        50   100   Active   local           192.168.50.2    192.168.50.1
Vl55        55   100   Active   local           192.168.55.2    192.168.55.1
MLS1-HQ#
```

```
MLS-HQ2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   90    Standby  192.168.10.3    local           192.168.10.1
Vl20        20   90    Standby  192.168.20.3    local           192.168.20.1
Vl30        30   90    Standby  192.168.30.3    local           192.168.30.1
Vl40        40   90    Standby  192.168.40.3    local           192.168.40.1
Vl50        50   90    Standby  192.168.50.3    local           192.168.50.1
Vl55        55   90    Standby  192.168.55.3    local           192.168.55.1
MLS-HQ2#
```

Figure 2.4: MLS1 & MLS2 HSRP verification.

```
router ospf 25
 router-id 1.2.1.2
 log-adjacency-changes
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
 network 192.168.50.0 0.0.0.255 area 0
 network 192.168.55.0 0.0.0.255 area 0
 network 192.168.255.0 0.0.0.3 area 0
!
router rip
!
ip classless
!

MLS1-HQ#
```

```
router ospf 25
 router-id 1.3.1.3
 log-adjacency-changes
 network 10.30.10.8 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
 network 192.168.50.0 0.0.0.255 area 0
 network 192.168.55.0 0.0.0.255 area 0
 network 192.168.255.248 0.0.0.3 area 0
```

Figure 2.5: MLS1 & MLS2 ospf verification with 1.2.1.2 & 1.3.1.3 as their respective router-ids

EtherChannel Configuration & Verification

Etherchannel Configuration

```
en
configure terminal
int range fa0/22-24
channel-group 1 mode active

int port-channel 1
switchport mode trunk
```

Figure 2.6: Etherchannel configuration between the multilayer switches.

```
MLS1-HQ#sh etherchannel po
MLS1-HQ#sh etherchannel port-channel ?
  <cr>
MLS1-HQ#sh etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 00d:02h:57m:13s
Logical slot/port   = 2/1       Number of ports = 3
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/22   Active             0
  0     00     Fa0/24   Active             0
  0     00     Fa0/23   Active             0
Time since last port bundled:    00d:02h:57m:13s    Fa0/23
Group: 2
```

```
MLS-HQ2>en
Password:
MLS-HQ2#sh ether
MLS-HQ2#sh etherchannel por
MLS-HQ2#sh etherchannel port-channel 1
                                ^
% Invalid input detected at '^' marker.

MLS-HQ2#sh etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 00d:02h:59m:00s
Logical slot/port   = 2/1       Number of ports = 3
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/24   Active             0
  0     00     Fa0/23   Active             0
  0     00     Fa0/22   Active             0
Time since last port bundled:    00d:02h:59m:00s    Fa0/22
MLS-HQ2#
```

Figure 2.7: Verification of EtherChannel created between the two multilayer switches.

Router OSPF and NAT configuration

```
WAN#sh ip ospf
 Routing Process "ospf 25" with ID 1.4.1.4
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an area border router
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 2. 2 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm executed 20 times
        Area ranges are
        Number of LSA 14. Checksum Sum 0x07782b
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 3
        Number of interfaces in this area is 0
        Area has no authentication
        SPF algorithm executed 3 times
        Area ranges are
        Number of LSA 15. Checksum Sum 0x06b0c4
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

WAN#
WAN#
WAN#
WAN#sh ip ospf ne
WAN#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
1.2.1.2           1   FULL/BDR        00:00:36    192.168.255.2   GigabitEthernet0/0
1.3.1.3           1   FULL/BDR        00:00:37    192.168.255.250 GigabitEthernet0/2
10.30.10.1        0   FULL/  -        00:00:33    10.30.10.1      Serial0/0/0
WAN#
```

Figure 2.8: HQ WAN router OSPF verification.

DHCP Pools & Verification

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
vlan20serverpool	192.168.20.1	0.0.0.0	192.168.20.4	255.255.255.0	240	0.0.0.0	0.0.0.0
vlan50serverpool	192.168.50.1	0.0.0.0	192.168.50.4	255.255.255.0	240	0.0.0.0	0.0.0.0
vlan40serverpool	192.168.40.1	0.0.0.0	192.168.40.4	255.255.255.0	240	0.0.0.0	0.0.0.0
vlan30serverpool	192.168.30.1	0.0.0.0	192.168.30.4	255.255.255.0	240	0.0.0.0	0.0.0.0
vlan10serverpool	192.168.10.1	0.0.0.0	192.168.10.4	255.255.255.0	240	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.55.0	255.255.255.0	512	0.0.0.0	0.0.0.0

Figure 2.9: DHCP pool of IP addresses for leasing for each subnet.

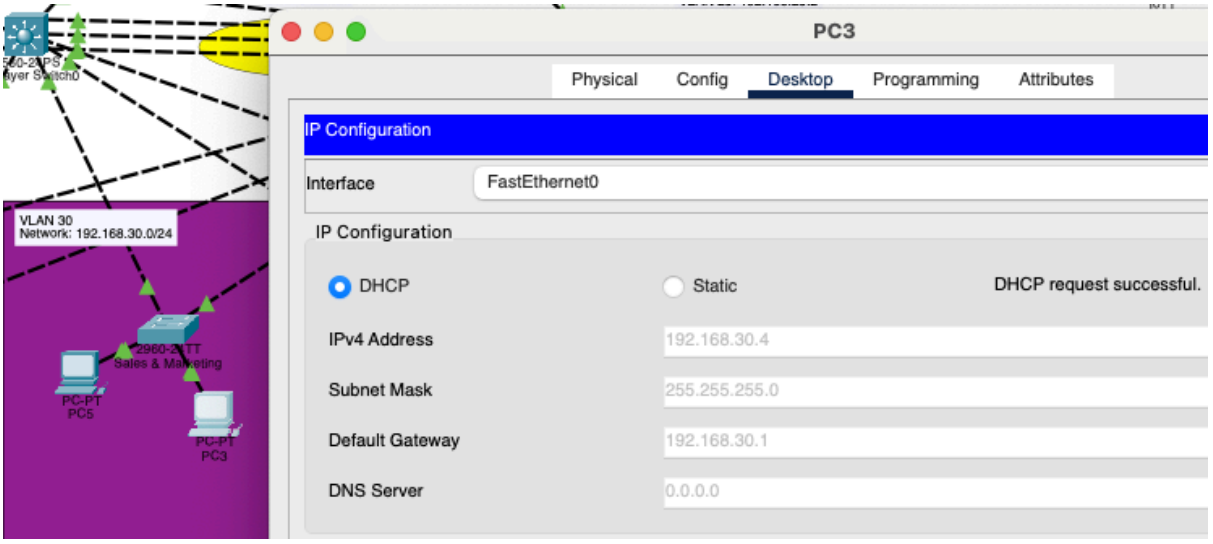
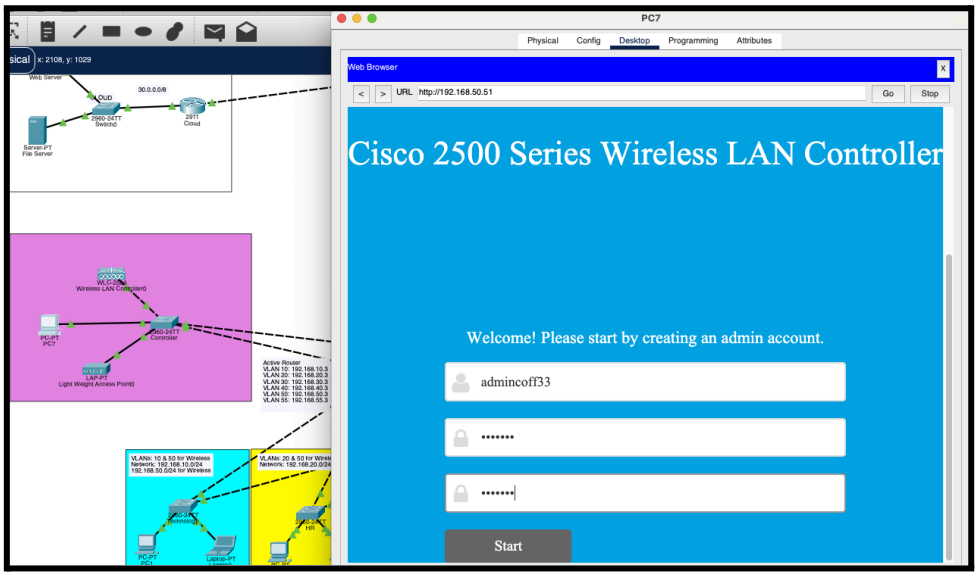
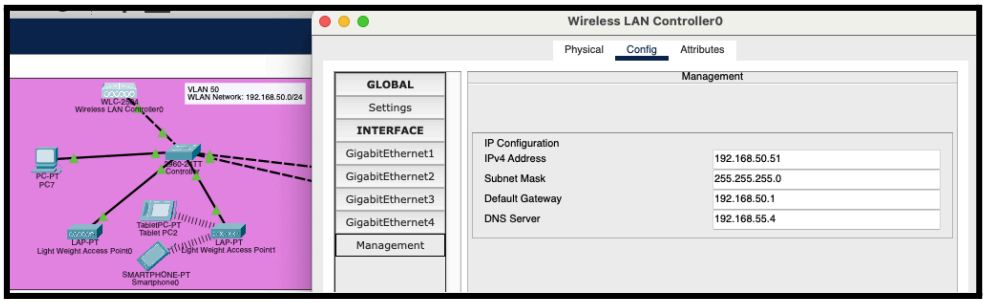


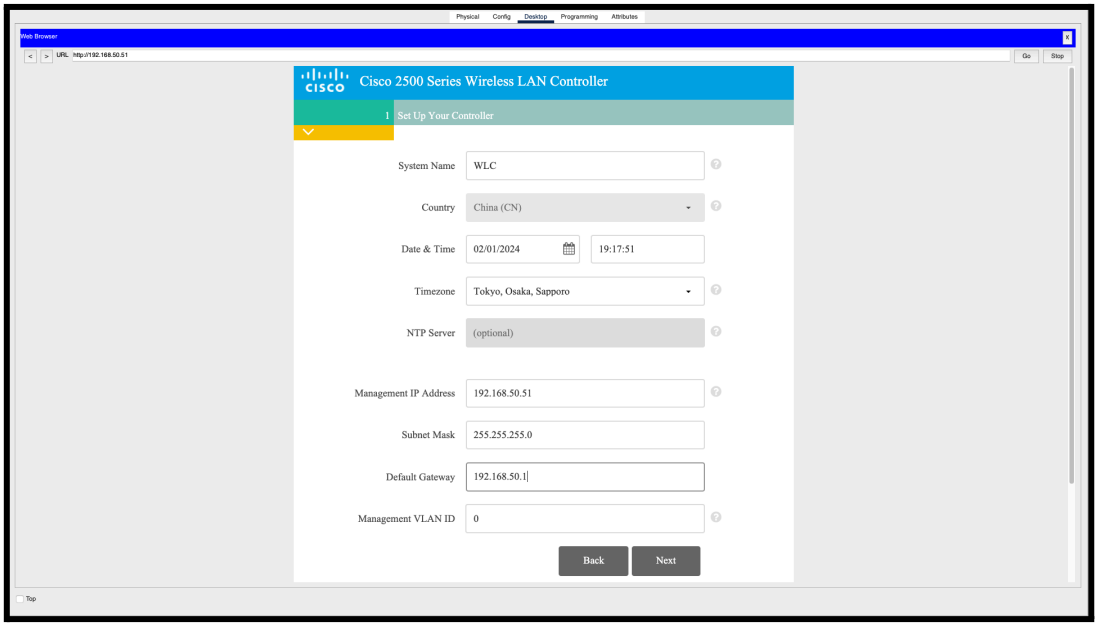
Figure 2.10: Verification and successful assignment of IP address by DHCP server.

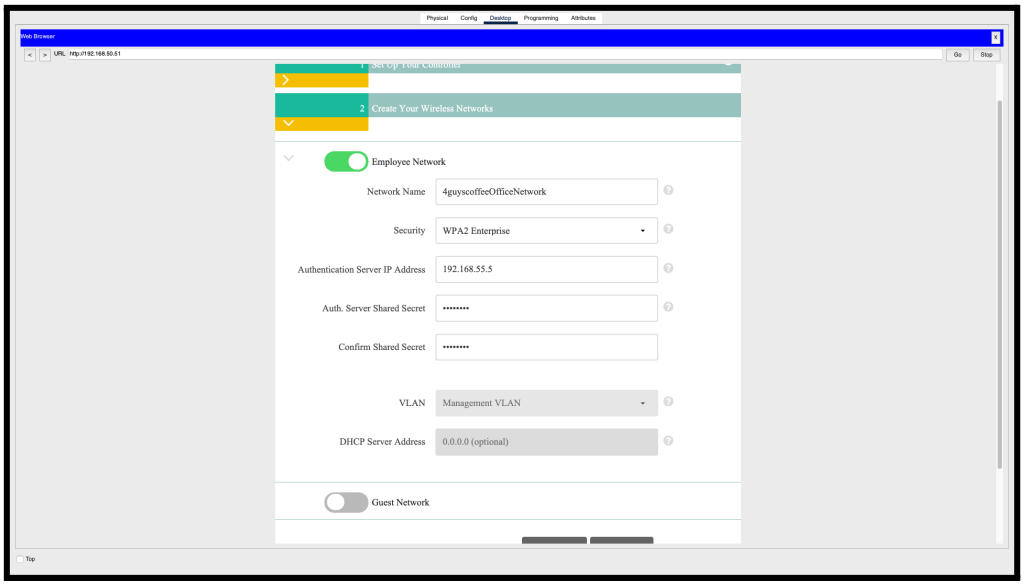
WLC Configuration & RADIUS Server Authentication

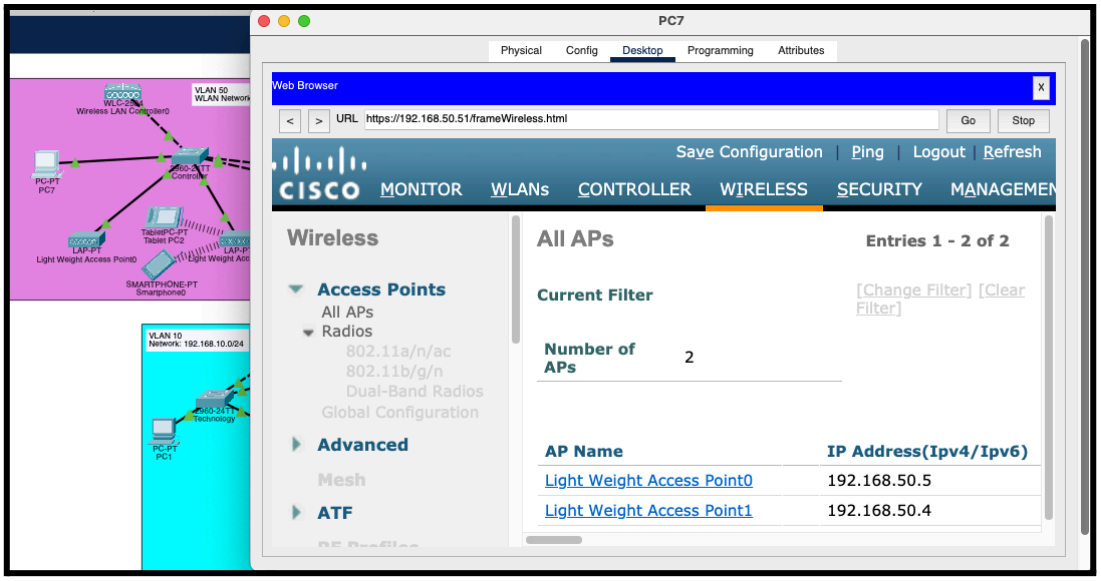
We have set up a WLC to manage our WLAN, which is also scalable, should additional networks be added. As seen from the screenshots below, there are two access points on the configuration web page and our leading network, 4guyscoffeeOfficeNetwork. WLCs provide an added layer of security to APs by providing authentication at a higher level, detecting rogue devices, and protecting the network behind a firewall. WLCs allow for centralised AP deployment. They simplify network maintenance operations. Also, we included a RADIUS server for authentication, requiring login credentials for staff users in the office HQ to access the wifi network instead of a wired connection.

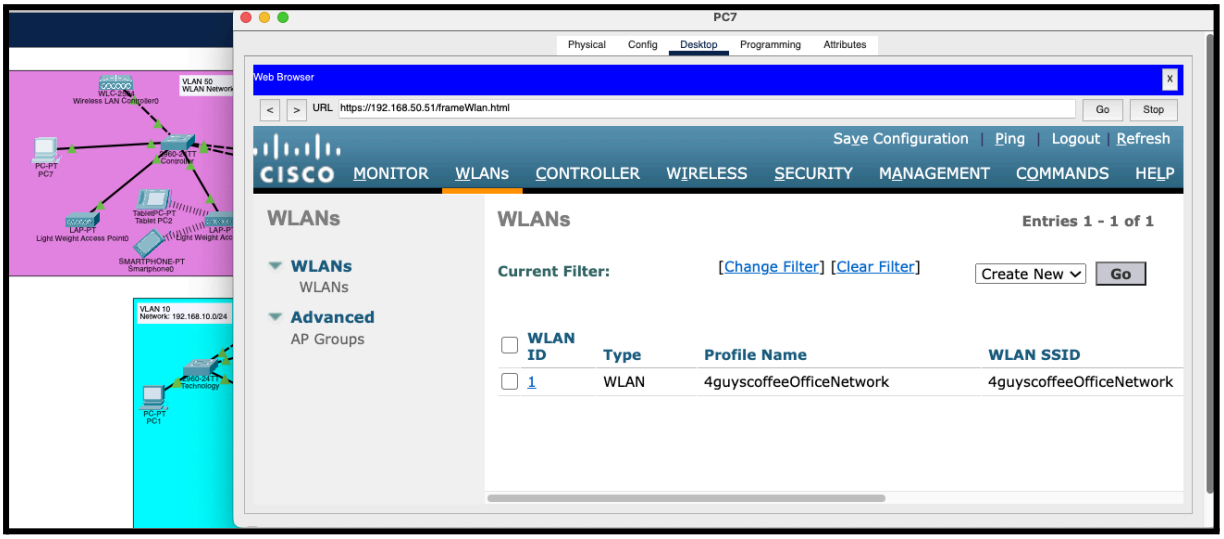



Wireless LAN Controller0
Physical
Config
Attributes
GLOBAL
Settings
INTERFACE
GigabitEthernet1
GigabitEthernet2
GigabitEthernet3
GigabitEthernet4
Management
Management
IP Configuration
IPv4 Address 192.168.50.51
Subnet Mask 255.255.255.0
Default Gateway 192.168.50.1
DNS Server 192.168.55.4
VLAN 50
WLAN Network: 192.168.50.0/24


Cisco 2500 Series Wireless LAN Controller
1 Set Up Your Controller
System Name WLC
Country China (CN)
Date & Time 02/01/2024 19:17:51
Timezone Tokyo, Osaka, Sapporo
NTP Server (optional)
Management IP Address 192.168.50.51
Subnet Mask 255.255.255.0
Default Gateway 192.168.50.1
Management VLAN ID 0
Back
Next


Create Your Wireless Networks
Employee Network
Network Name
4guyscoffeeOfficeNetwork
Security
WPA2 Enterprise
Authentication Server IP Address
192.168.55.5
Auth. Server Shared Secret
Confirm Shared Secret
VLAN
Management VLAN
DHCP Server Address
0.0.0.0 (optional)
Guest Network


PC7
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://192.168.50.51/frameWireless.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMEN
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
ATF
All APs
Entries 1 - 2 of 2
Current Filter
[Change Filter] [Clear Filter]
Number of APs
2
AP Name
IP Address(Ipv4/Ipv6)
Light Weight Access Point0
192.168.50.5
Light Weight Access Point1
192.168.50.4


PC7
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL https://192.168.50.51/frameWlan.html
Go
Stop
Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
WLANs
WLANs
WLANs
Advanced
AP Groups
Entries 1 - 1 of 1
Current Filter:
[Change Filter] [Clear Filter]
Create New
Go
WLAN ID
Type
Profile Name
WLAN SSID
1
WLAN
4guyscoffeeOfficeNetwork
4guyscoffeeOfficeNetwork

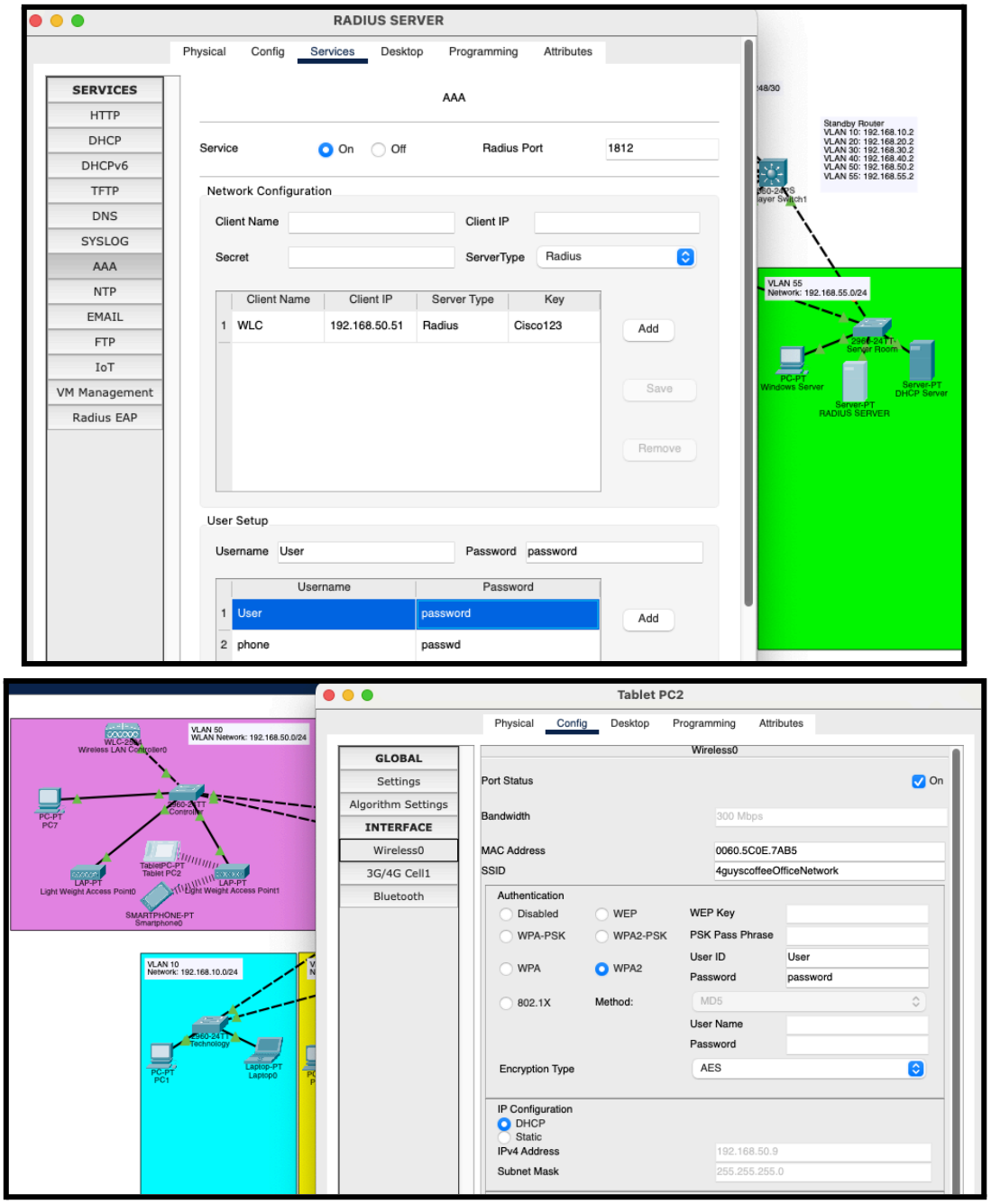


Figure 2.11-2.18: Series of screenshots for WLC and RADIUS server configuration.

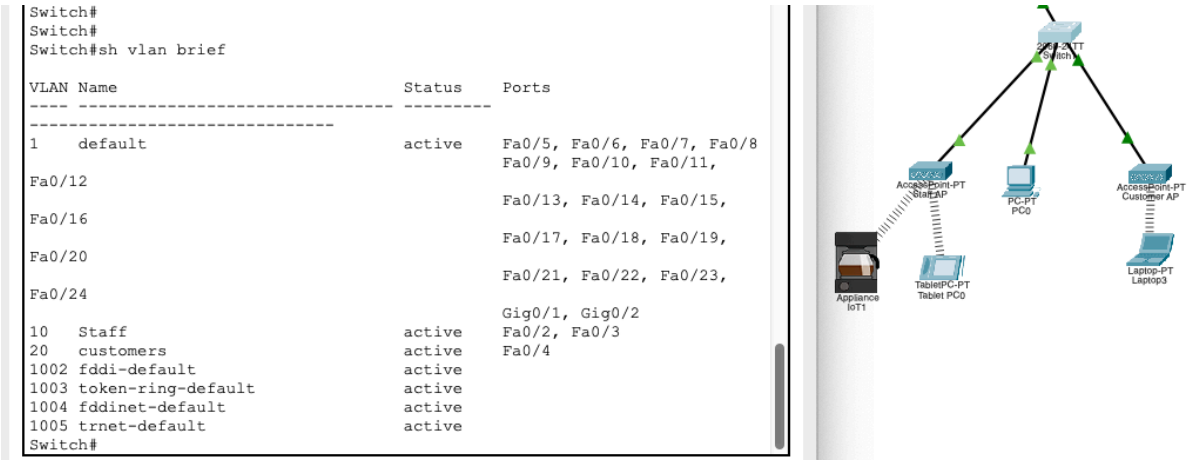
Branch - Switches & Routers

Our cafe branches are dine-in cafes with wifi access for customers to use. We have set up the cafe with separate access points, different VLANs, and networks for multilayered security. We used a simple router-on-a-stick topology to facilitate inter-vlan connectivity as it is simple to set up and use SVIs. Both network topology and configurations of the branches are similar.

Switch VLANs

Table 4: VLAN table for the switches in each branch.

VLAN	Name
10	Staff
20	Customers

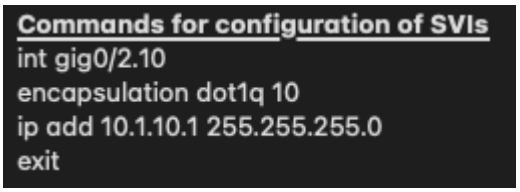


```
Switch#
Switch#
Switch#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11,
Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15,
Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19,
Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23,
Fa0/24
                                                 Gig0/1, Gig0/2
10   Staff                             active    Fa0/2, Fa0/3
20   customers                         active    Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Figure 2.19: Verification of the VLANs on the switches in the branches.

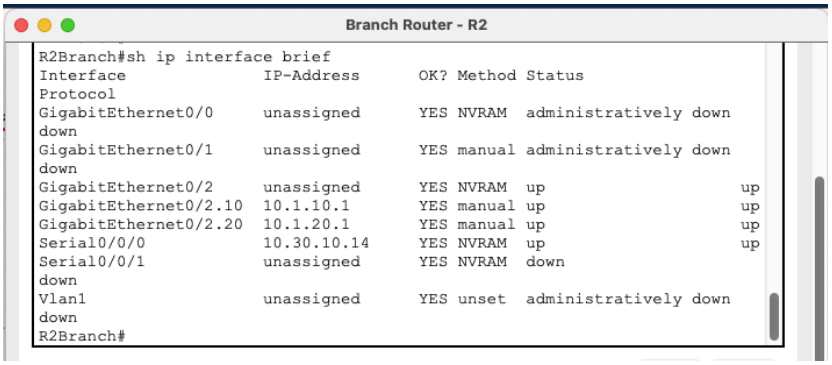
Router

SVIs on Router for Inter-VLAN routing



```
Commands for configuration of SVIs
int gig0/2.10
encapsulation dot1q 10
ip add 10.1.10.1 255.255.255.0
exit
```

Figure 2.20: Configuration commands for SVIs on Router.



```
Branch Router - R2

R2Branch#sh ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     unassigned      YES NVRAM  administratively down
down
GigabitEthernet0/1     unassigned      YES manual administratively down
down
GigabitEthernet0/2     unassigned      YES NVRAM  up                    up
GigabitEthernet0/2.10  10.1.10.1       YES manual up                    up
GigabitEthernet0/2.20  10.1.20.1       YES manual up                    up
Serial0/0/0            10.30.10.14     YES NVRAM  up                    up
Serial0/0/1            unassigned      YES NVRAM  down
down
Vlan1                  unassigned      YES unset  administratively down
down
R2Branch#
```

Figure 2.21: SVIs verification for branch router.

Router as DHCP

As it would be expensive to have a dedicated DHCP server for every branch, we have also configured the router branch to be a DHCP server.

```
Router DHCP configuration
ip dhcp pool 1
network 10.1.10.0 255.255.255.0
default-router 10.1.10.1
exit
ip dhcp excluded-address 10.1.10.1
ip dhcp pool 2
network 10.1.20.0 255.255.255.0
default-router 10.1.20.1
exit
ip dhcp excluded-address 10.1.20.1
```

Figure 2.22: Configuring branch router as DHCP server.

Figure 2.23: Router DHCP verification.

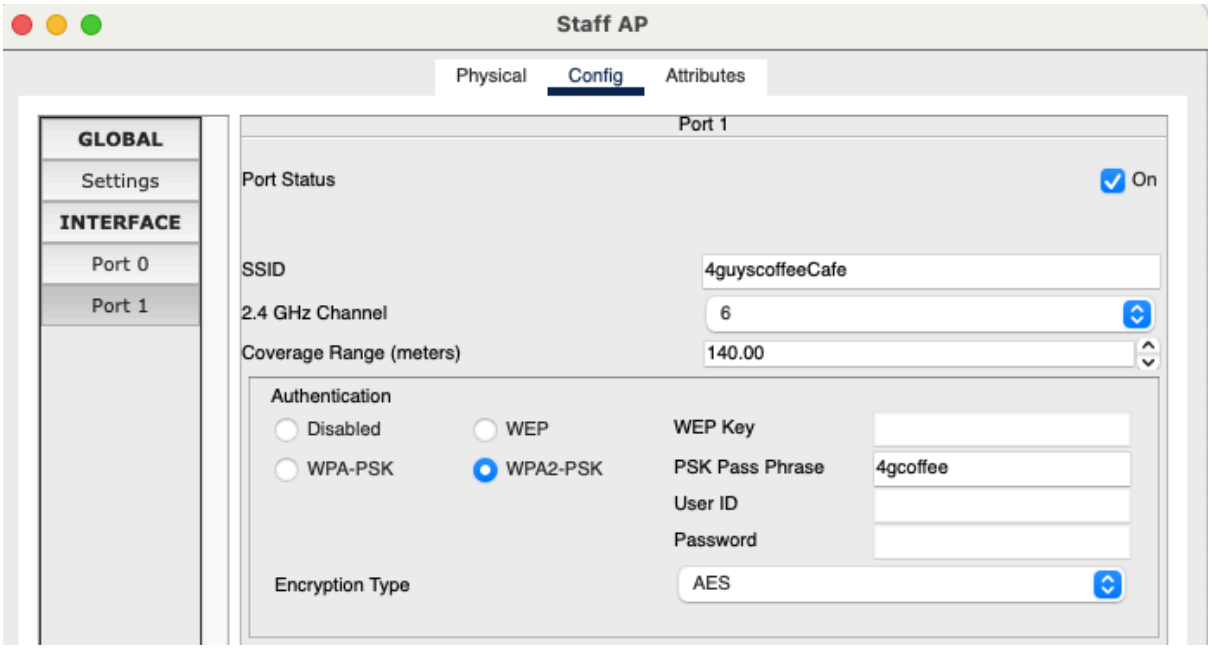
Router OSPF verification

```
R2Branch#sh ip ospf database
            OSPF Router with ID (10.30.10.12) (Process ID 25)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.30.10.12     10.30.10.12     382         0x8000000d 0x00bb7d 4
10.30.10.1      10.30.10.1      385         0x8000000f 0x006bcf 6
20.20.20.1      20.20.20.1      384         0x8000000d 0x00e5f7 4
1.4.1.4         1.4.1.4         353         0x80000010 0x00bb94 4
1.3.1.3         1.3.1.3         344         0x80000017 0x00560b 7
1.2.1.2         1.2.1.2         341         0x80000017 0x002031 7

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.55.2    1.3.1.3         354         0x80000029 0x005229
192.168.255.1   1.4.1.4         353         0x80000011 0x00efd7
192.168.255.249 1.4.1.4         353         0x80000012 0x003e8d
192.168.50.2    1.3.1.3         349         0x8000002a 0x0087f7
192.168.20.2    1.3.1.3         349         0x8000002b 0x00d0cb
192.168.10.2    1.3.1.3         349         0x8000002c 0x003d68
192.168.40.3    1.2.1.2         346         0x80000009 0x003477
192.168.30.2    1.3.1.3         344         0x8000002d 0x005e32
R2Branch#
```

Figure 2.24: OSPF database of branch router.

Access Points Configuration

We made use of WPA2-PSK for security encryption for both staff and customer use at each access point.



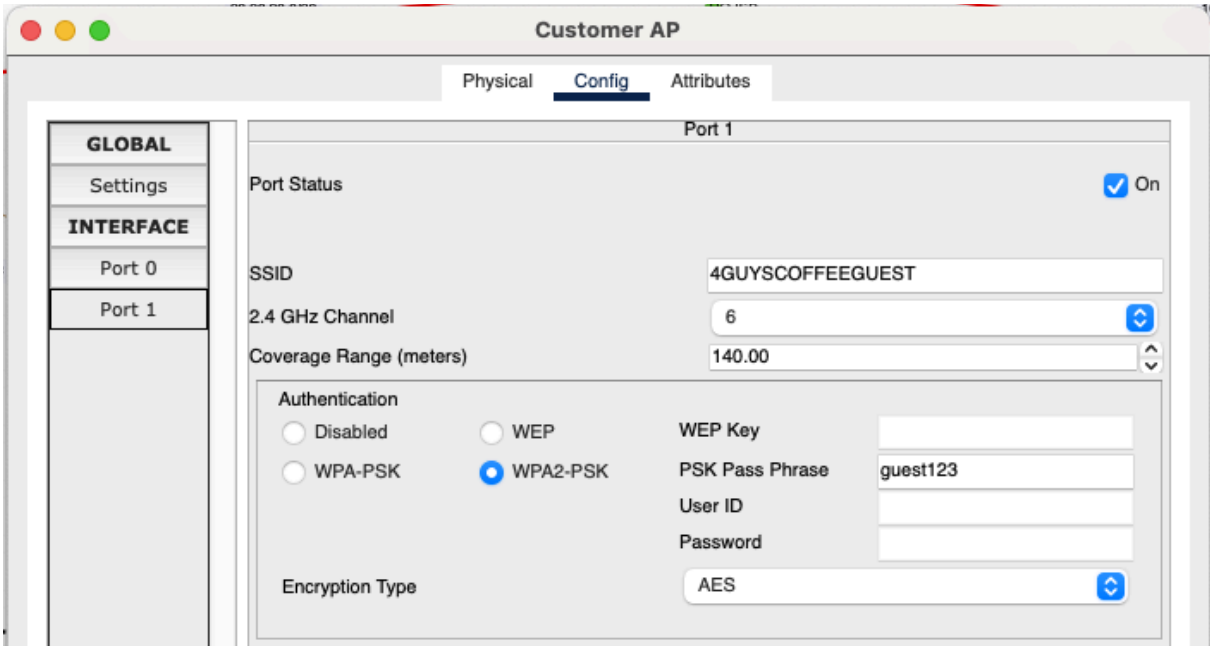


Figure 2.25-2.26: APs configuration for branch cafes with WPA2-passkey.

Connectivity

Connectivity between different VLANs

HQ LAN

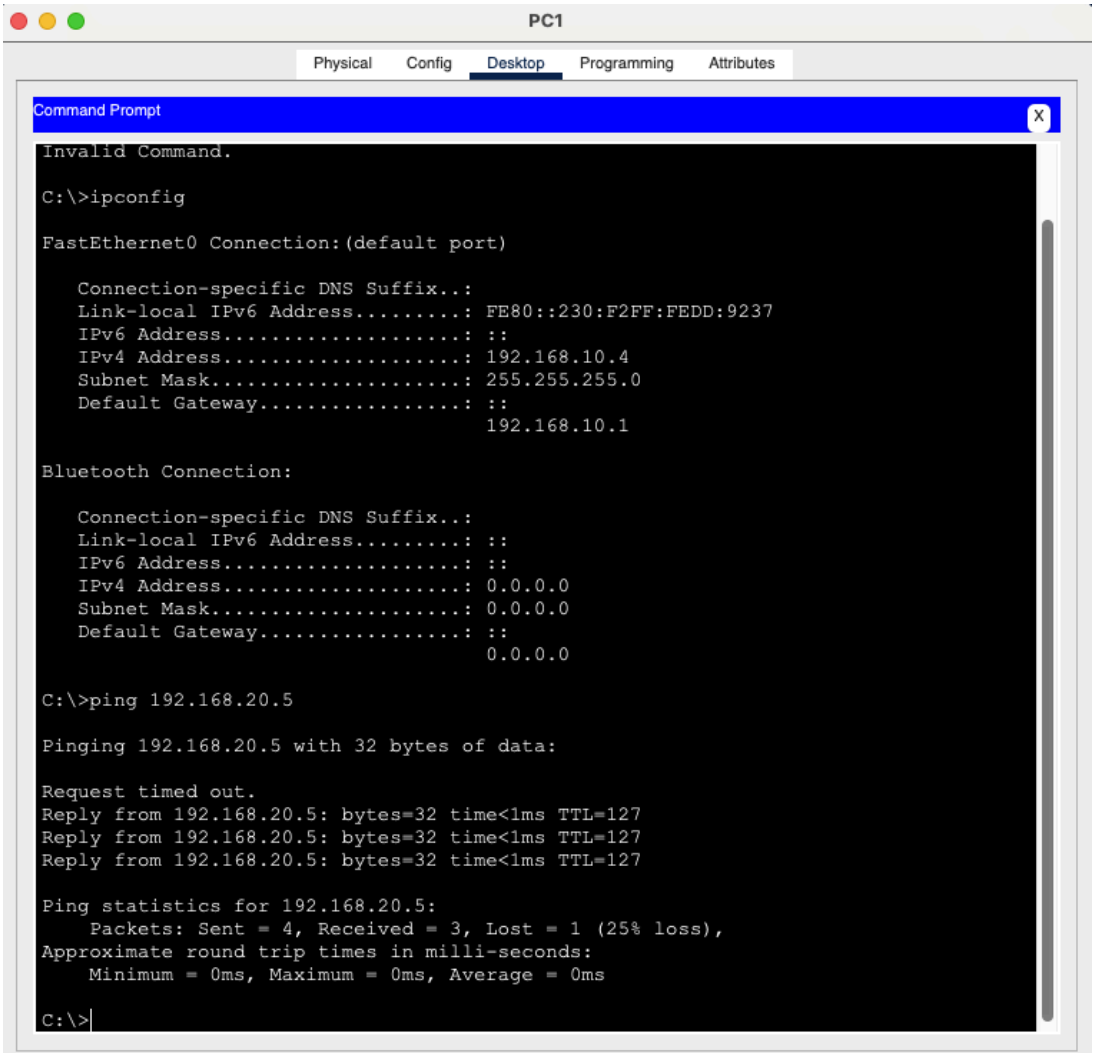


Figure 2.27: Pinging from a PC in Technology, VLAN 10 to a PC in HR, VLAN 20.

Branch LAN

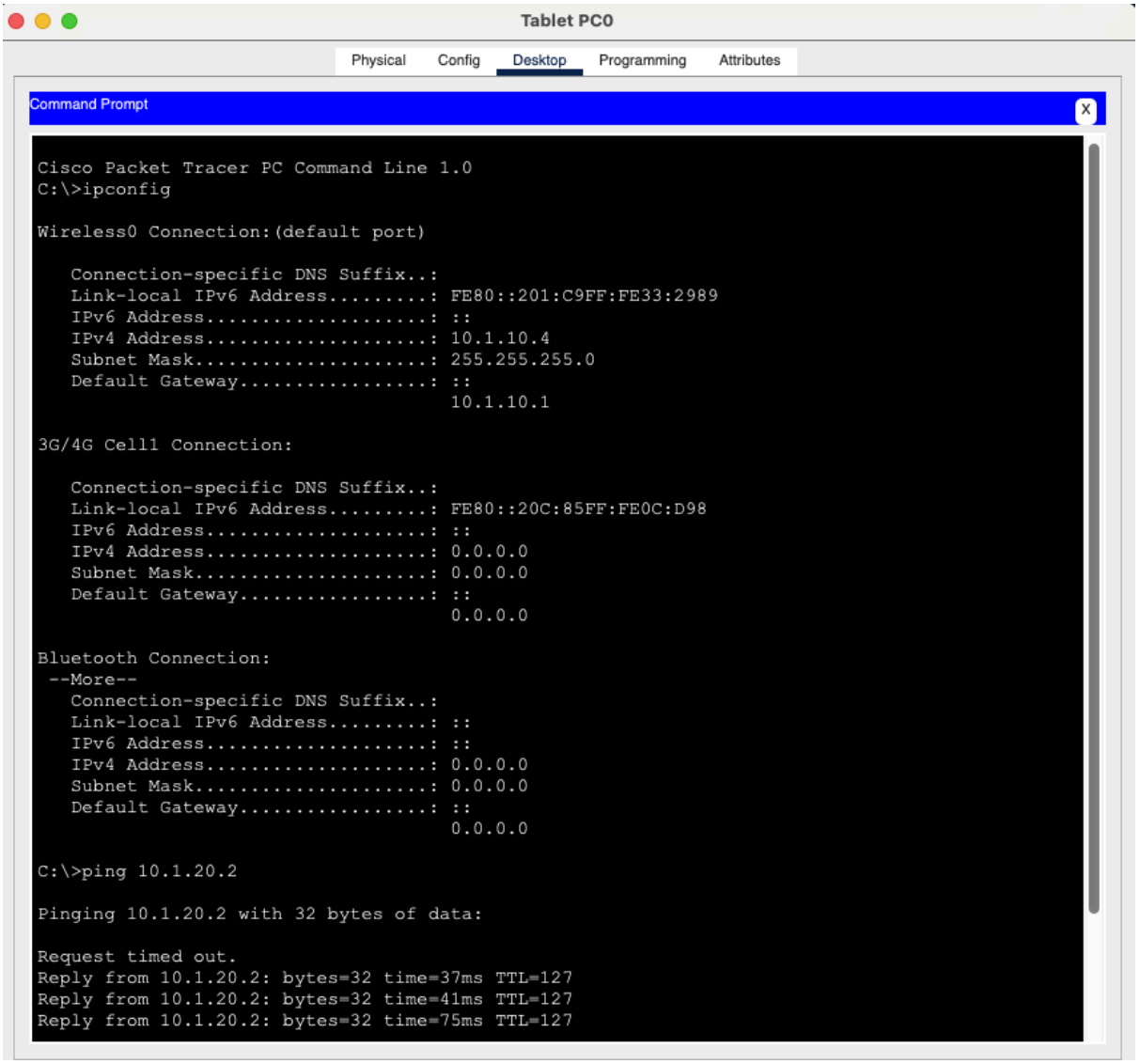


Figure 2.28: Pinging from a tablet connected to the staff AP, VLAN 10, to a customer laptop connected to the customer AP, VLAN 20.

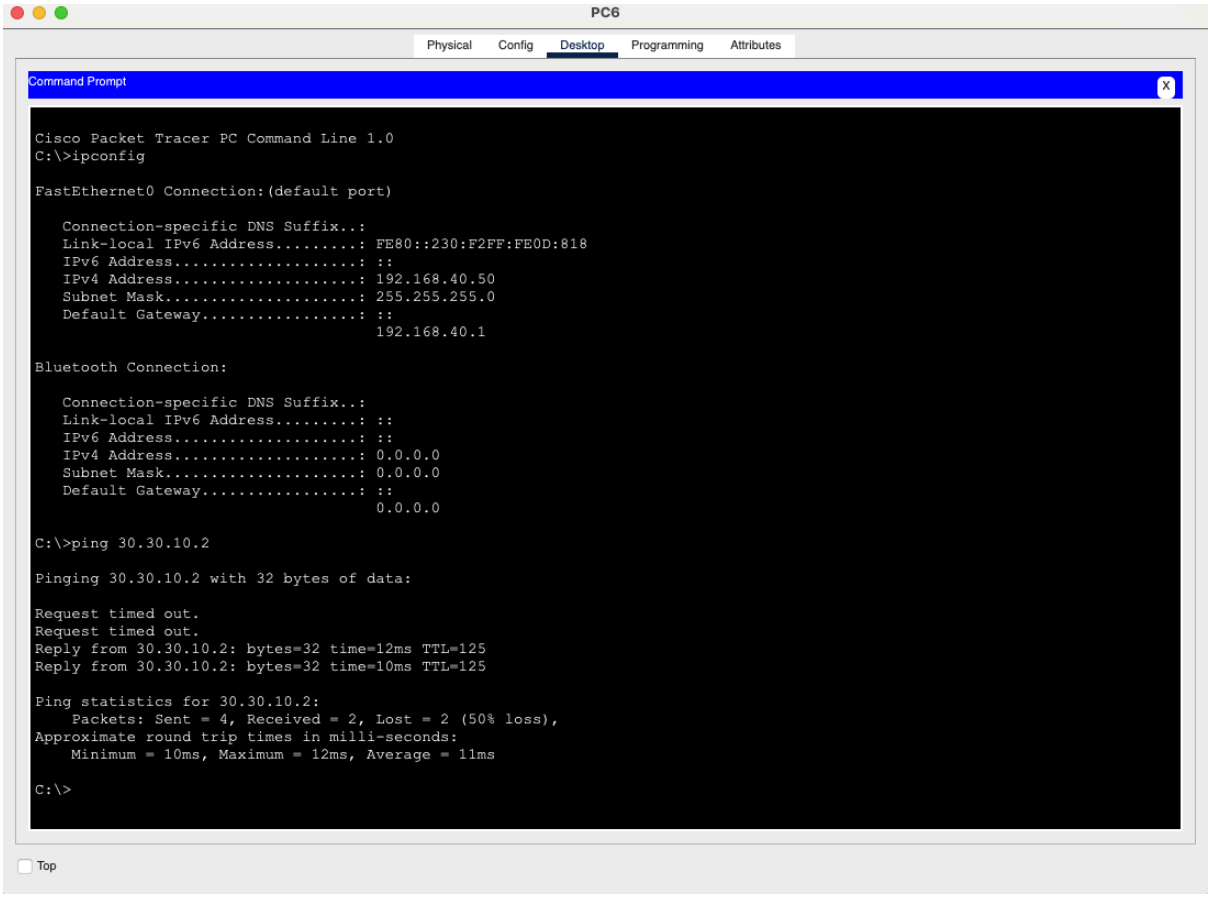


Figure 2.29: Pinging from HQ to Orchard Branch's PC.

Site-to-site VPN

Configuration of VPN

VPN Configuration

Step 1: Check if they have the security package installed in one of the geographical routers:
show version

Step 2: Install the package if it shows disabled
license boot module c2900 technology-package securityk9

Step 3: Create an extended access list to permit traffic to the specific interface of the branch.
access-list 100 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.255.255

Step 4: Create the IPsec tunnel and bind to interface
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key vpn address 10.30.10.14
crypto ipsec transform-set VPN-P2 esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
description VPN connection to R3
set peer 10.30.10.14
set transform-set VPN-P2
match address 100
exit
interface se0/0/0
crypto map VPN-MAP

Step 5: Repeat for the other branch router.

Figure 2.30: VPN tunnel configuration between 2 sites.

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            disable       None          None
data          disable       None          None

Configuration register is 0x2102


WAN#
```

Figure 2.31: Security package installed - ‘Evaluation’.

```
WAN#show ac
WAN#show access-lists
Extended IP access list 100
    10 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.255.255
Extended IP access list 150
    10 permit ip 192.168.0.0 0.0.255.255 30.30.0.0 0.0.255.255 (1 match(es))

WAN#
```

Figure 2.32: Access List verification for VPN.

VPN verification

```
WAN#
WAN#
WAN#
WAN#sh cry
WAN#sh crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP2, local addr 10.30.10.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port): (30.30.0.0/255.255.0.0/0/0)
   current_peer 20.20.20.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
   #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.30.10.2, remote crypto endpt.:20.20.20.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xEE5B9B9C(3998981020)

     inbound esp sas:
      spi: 0xBE16AC84(3189156996)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2000, flow_id: FPGA:1, crypto map: VPN-MAP2
        sa timing: remaining key lifetime (k/sec): (4525504/2619)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xEE5B9B9C(3998981020)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: FPGA:1, crypto map: VPN-MAP2
        sa timing: remaining key lifetime (k/sec): (4525504/2619)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Figure 2.33: Verification that a tunnel has been formed between the two sites and packets are encrypted after a successful ping.

2. Windows & Linux Server Administration

Microsoft Active Directory

This section functions as an exhaustive guide delineating our strategic approach to harnessing the capabilities of Active Directory, elucidating the meticulous procedures we have undertaken to establish a resilient and secure directory service within our organisation. The implementation of Active Directory is paramount in our pursuit of constructing a centralised and methodically organised network, proficiently managing user accounts, facilitating seamless resource access, and ensuring a secure and scalable operational environment.
In an unwavering commitment to fortifying data security, we have instituted stringent measures to mitigate potential threats proactively, safeguard sensitive information, and uphold the integrity of our systems. Our adoption of a dual-server approach underscores our steadfast dedication to delivering a seamless and secure digital ecosystem.
A dedicated PC setup has been established within each cafe to address the operational requisites of our branch managers, particularly those overseeing our cafe outlets. Leveraging a secure Virtual Private Network (VPN) connection, these branch managers can seamlessly access the central file server located at the head office. This robust infrastructure enables the swift retrieval of Point-of-Sale (POS) materials and other critical information, fostering a cohesive and responsive network environment.

AD Installation

Active Directory Domain Services (AD DS) is a critical component in Windows Server environments, and several vital functionalities and benefits underscore its importance.
The Installation Video documents the steps to ensure the AD DS runs correctly.

Brief steps:

1. Prepare the Server
2. Add Roles and Features
3. Install AD DS
4. Promote the Server to a Domain Controller
5. Active Directory Domain Services Configuration Wizard

Post-Installation Notes:

1. Verify Active Directory Installation
2. Backup:
    - Regularly back up the domain controller, especially the Active Directory database.
3. (Optional) We strongly recommend adding extra domain controllers (DC). We will undertake these steps:
    - Configure the Static IP for the new PC.
    - As for DNS, ensure it is set according to the DNS address of the primary DC.

- Add AD DS and DHCP roles as guided in previous steps.
- Promote the new PC as a Domain Controller.
- Flexible Single Master Operation or FSMO roles can also be configured using the Active Directory Users and Computers tool.
- Tip: The current FSMO roles can be determined by running this command in the command prompt: [netdom query fsmo]

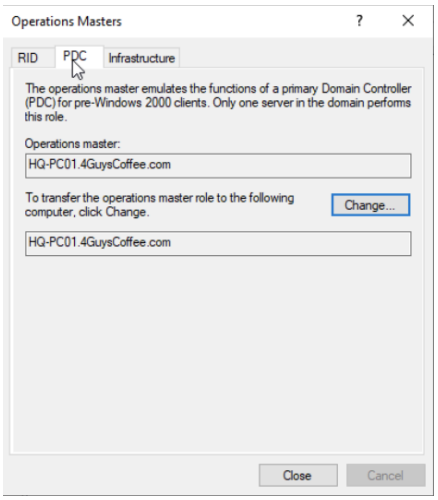


Figure 3.1: Delegating the Operations Masters

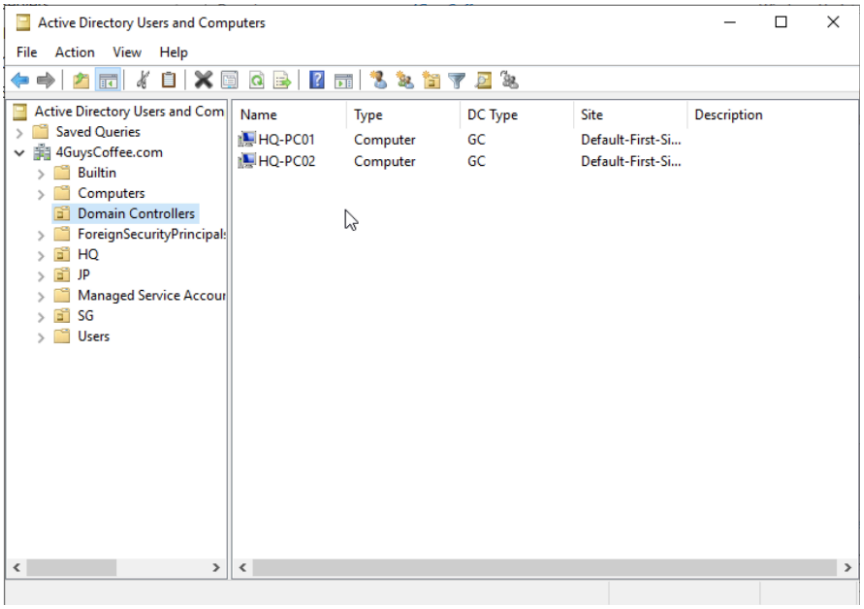


Figure 3.2: Domain Controllers

Adding Organizational Units

Ensuring the security of our Active Directory is paramount in upholding our network's integrity and confidentiality. As a preliminary measure in establishing our comprehensive security protocols, we initiate the process by systematically classifying our branches, departments, and users into distinct Organizational Units (OU). This pivotal step empowers our System Administrators to methodically delegate specific administrative tasks to individuals or groups within a designated OU. Significantly, this approach facilitates the distribution of administrative responsibilities, bolstering security measures by restricting access solely to essential components.

Given the expansive nature of our workforce, we have implemented a PowerShell script to automate the creation of user accounts based on the employee list provided by our HR team. This script intelligently categorises employees into their respective departments, mitigating the potential for unforeseen anomalies and human errors. Beyond immediate benefits, such automation is a proactive measure, efficiently saving time in the face of future team changes. This streamlined approach underscores our commitment to precision, efficiency, and sustained security within our Active Directory infrastructure.

FirstName	Initials	LastName	UserName	Email	Street Address	City	Country	Department	JobTitle
Rahul	RK	Kapoor	rahul.kapoor	rahul.kapoor@4GuysCoffee.com		Singapore	SG	HQ	General Manager
Aditya	AM	Malhotra	aditya.malhotra	aditya.malhotra@4GuysCoffee.com		Singapore	SG	Cafe	Branch Manager
Li Hua	LO	Ong	lihua.ong	lihua.ong@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Lorna	LR	Rodriguez	lorna.rodriguez	lorna.rodriguez@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Aryan	AS	Singh	aryan.singh	aryan.singh@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Sofia	SH	Harun	sofia.harun	sofia.harun@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Li Yan	LH	Ho	liyan.ho	liyan.ho@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Rajiv	RP	Pillai	rajiv.pillai	rajiv.pillai@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Carlo	CV	Villanueva	carlo.villanueva	carlo.villanueva@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Irfan	IS	Shah	irfan.shah	irfan.shah@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Si Ling	ST	Toh	siling.toh	siling.toh@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Arif	AH	Hakim	arif.hakim	arif.hakim@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Aisha	AT	Tan	aisha.tan	aisha.tan@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Cristine	CR	Reyes	cristine.reyes	cristine.reyes@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Anjali	AK	Khanna	anjali.khanna	anjali.khanna@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Eliza	EI	Ismail	eliza.ismail	eliza.ismail@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Maricar	MA	Abad	maricar.abad	maricar.abad@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Omar	OK	Khairi	omar.khairi	omar.khairi@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Sebastian	SZ	Zhou	sebastian.zhou	sebastian.zhou@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Angela	AV	Valdez	angela.valdez	angela.valdez@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Zayd	ZF	Faris	zayd.faris	zayd.faris@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Vincent	VL	Lim	vincent.lim	vincent.lim@4GuysCoffee.com		Singapore	SG	Cafe	Branch Manager
Sabrina	SW	Wong	sabrina.wong	sabrina.wong@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Renato	RC	Cruz	renato.cruz	renato.cruz@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Danish	DF	Farhan	danish.farhan	danish.farhan@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
James	JL	Low	james.low	james.low@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Adrian	AL	Lim	adrian.lim	adrian.lim@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Alia	AH	Hanafi	alia.hanafi	alia.hanafi@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Shallop	SZ	Zhang	shallop.zhang	shallop.zhang@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Jessica	JH	Huang	jessica.huang	jessica.huang@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff
Arnav	AK	Khurana	arnav.khurana	arnav.khurana@4GuysCoffee.com		Singapore	SG	Cafe	Cafe Staff

Figure 3.3: A CSV file sent by our HR team containing the credentials of our staff

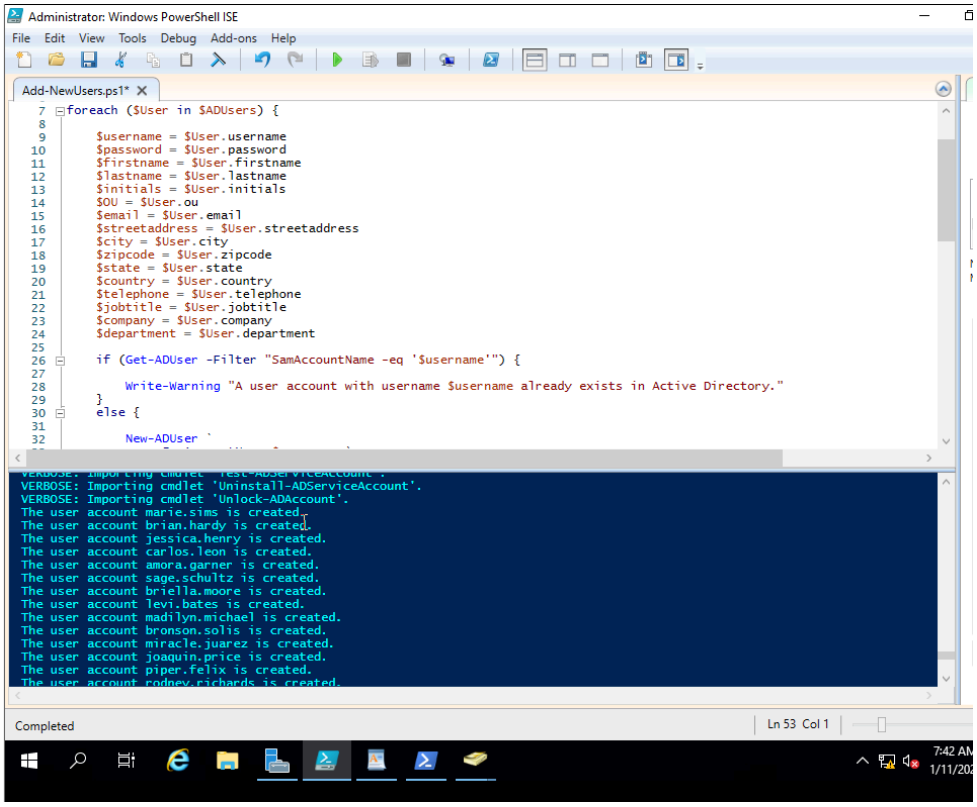


Figure 3.4: An excerpt of the Script to Automate the Account Creation of Our Staff

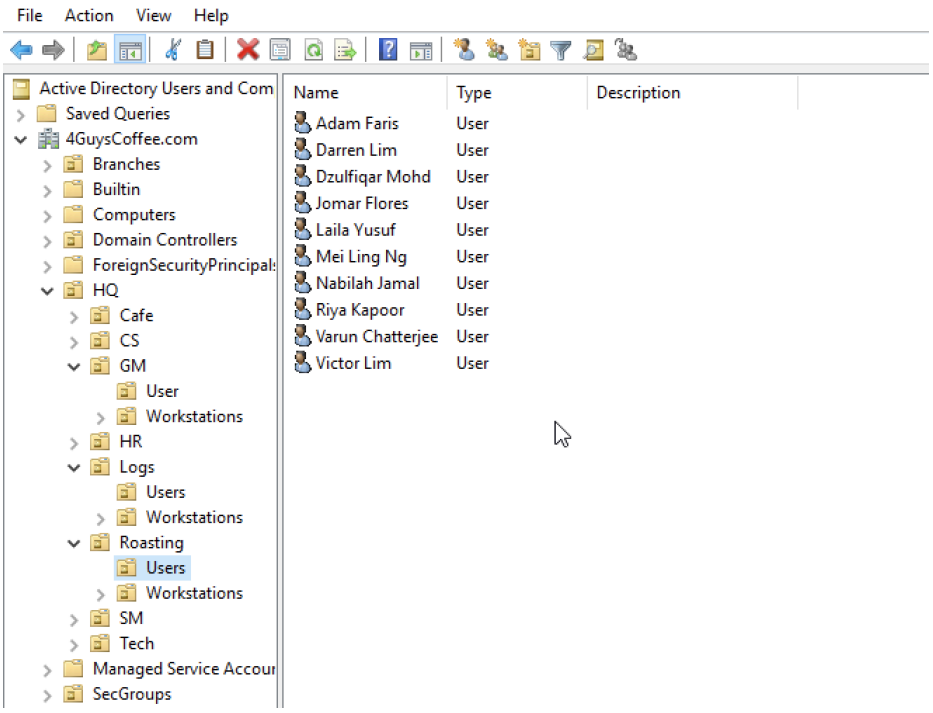


Figure 3.5: 161 Staff added to their respective departments

Creating Security Groups & Enabling File-Sharing

Next, we create security groups to efficiently manage and enforce access controls within our networked environment. This enables our System Administrators to logically organise and assign permissions to users based on their roles or responsibilities. By associating users with specific security groups, file sharing becomes a streamlined process, ensuring that only authorised individuals can access sensitive information. This enhances data security and simplifies administration by allowing permissions to be managed at the group level rather than individually for each user.

Overall, security groups, in conjunction with file sharing through AD, provide a robust framework for implementing a least privileged access model, minimising the risk of unauthorised access and enhancing the overall security posture of the network environment.

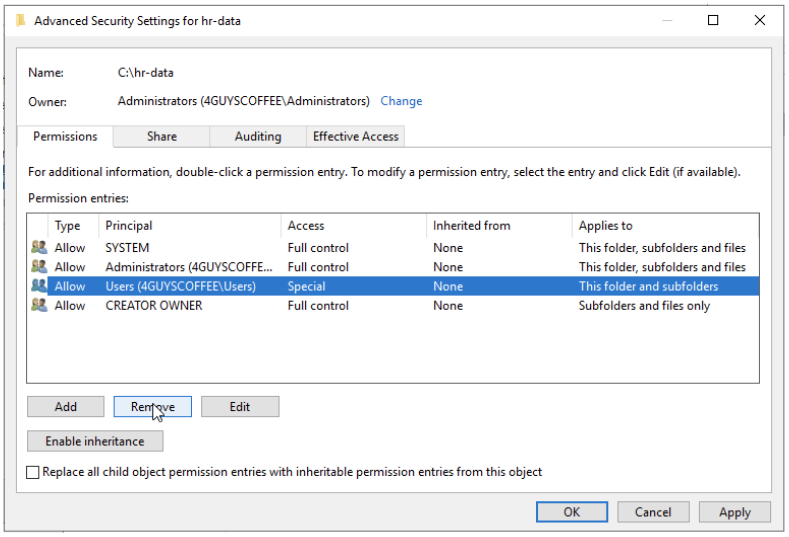


Figure 3.6: Removal of Domain Users from the Permission Entries (to Secure Confidential Files)

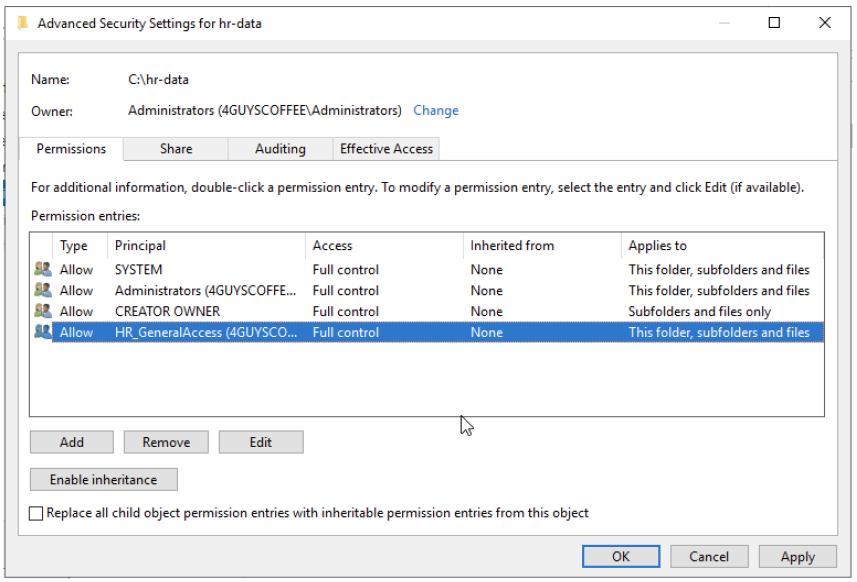


Figure 3.7: Adding a Security Group to the Entry

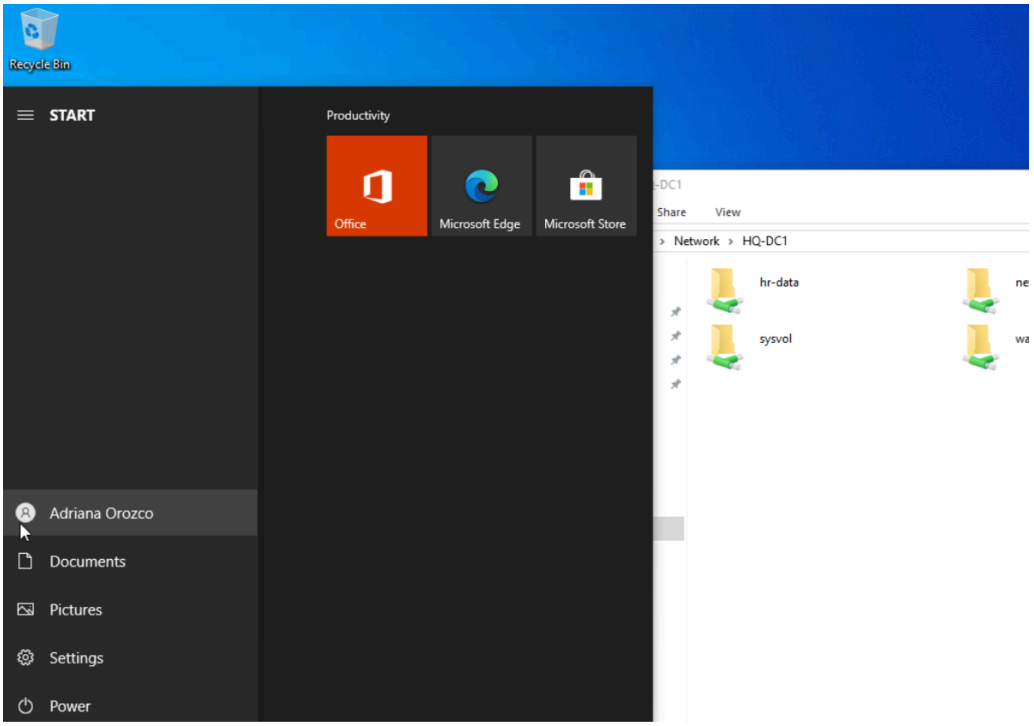


Figure 3.8: Our HR (Orozco) Account Successfully Accessing The Shared Folder

Security Measures

Now that we have created our OUs and Security Groups, here are some of the measures that we have implemented to take our security to the next level:

1. Group Policy Objects (GPOs) to enforce security settings such as password policies (enforce strong passwords, length of the passwords, expiration, etc), and user rights assignments.

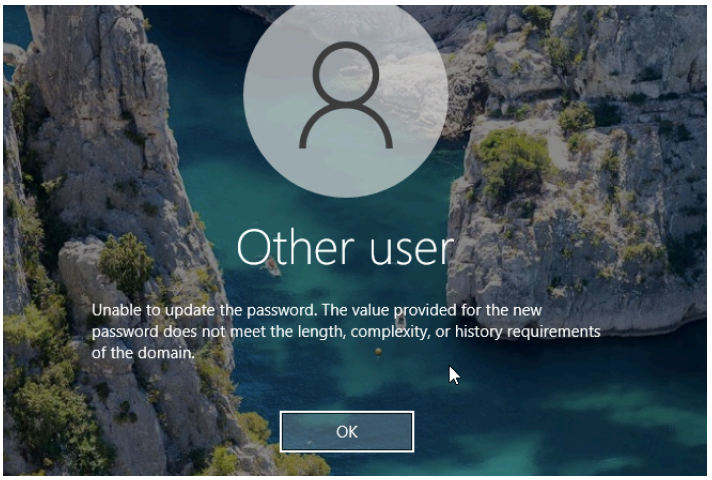


Figure 3.9: Stringent Password Policies Being Enforced

2. Account lockout policies to limit login attempts and protect against brute-force attacks.

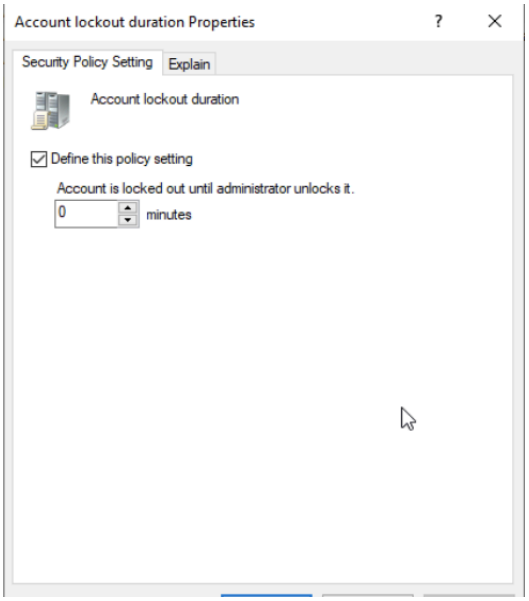


Figure 3.10: Setting the Account Lockout Duration

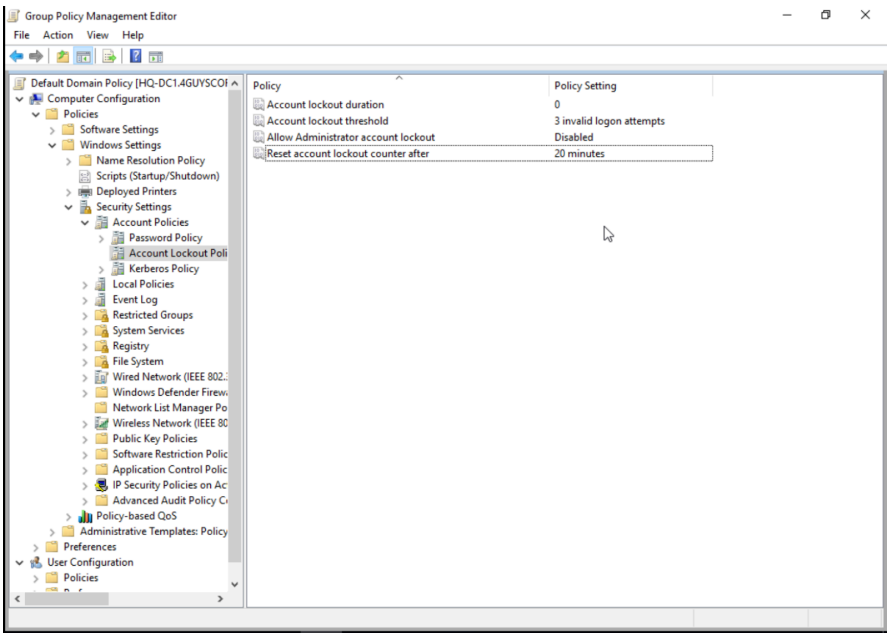


Figure 3.11: Account Lockout Configuration

3. We have configured the GPO rules to turn the firewalls on automatically in all of our workstations and disallow users to disable them. **Demonstration Video**

4. Inbound firewall rules allow only essential traffic to our domain controllers, limit unnecessary ports and services and implement outbound firewall rules to restrict unnecessary communication from domain controllers. **Demonstration Video**

5. Implement regular updates, scanning and patching to address vulnerabilities promptly.

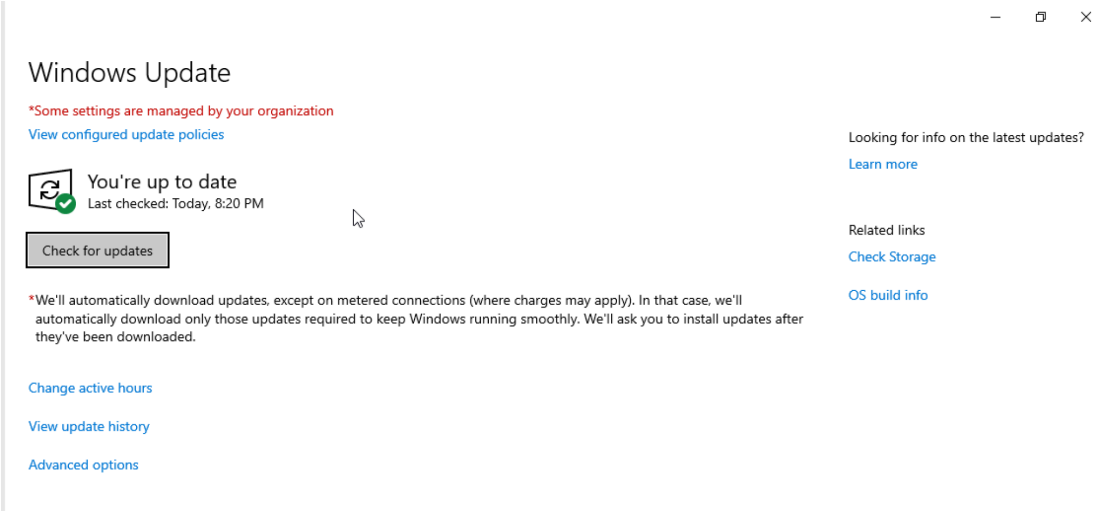


Figure 3.12: Updated Windows

Figure 3.13: Virus & Threat Scanning

6. Disable insecure protocols like SMB1.

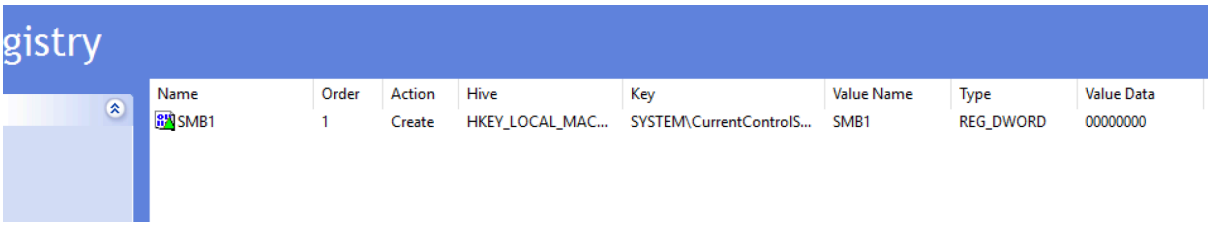


Figure 3.14: Creating a New Registry via GPO to Disable SMB Protocol 1

7. Disable Link-Local Multicast Name Resolution (LLMNR) via GPO.

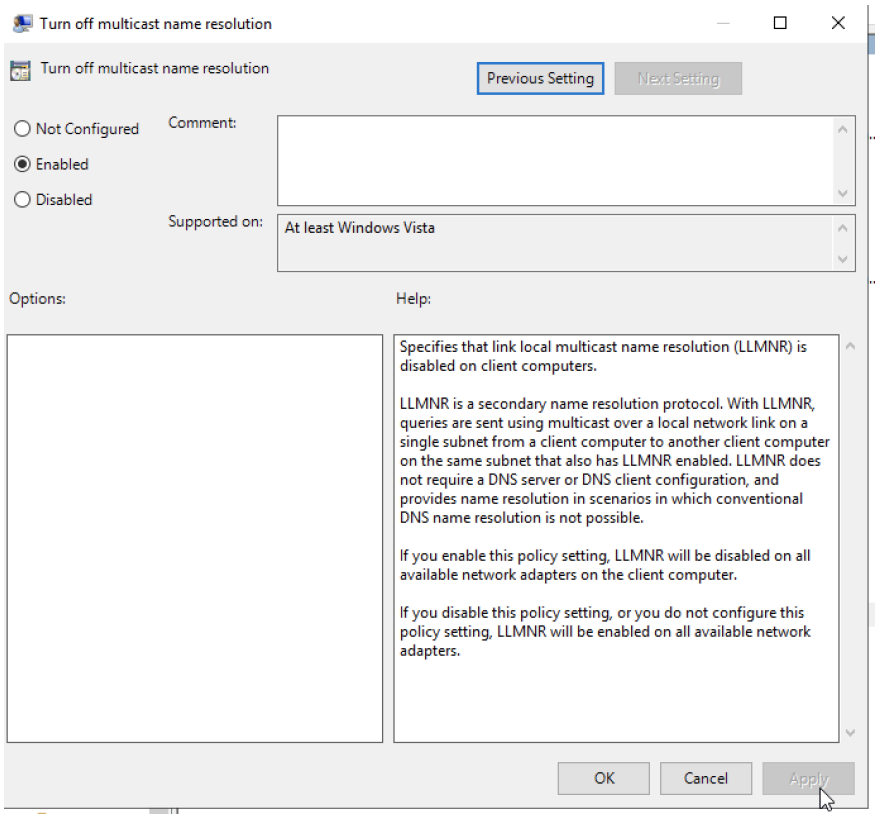


Figure 3.15: Disabled LLMNR

8. Disable NetBIOS Name Service (NBT-NS) via PowerShell.

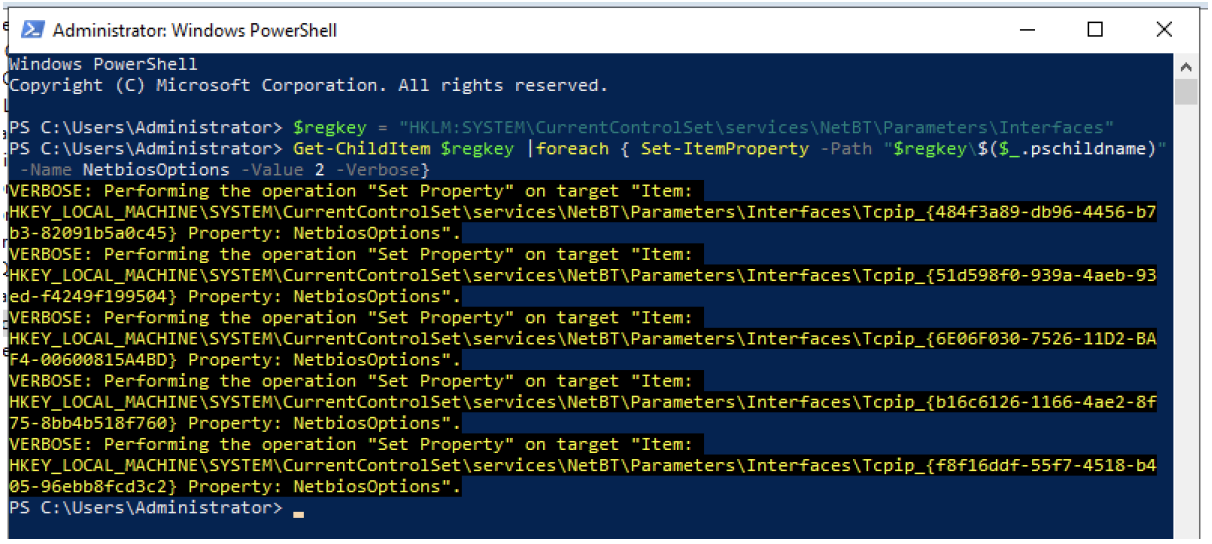


Figure 3.16: Edited Registry via PowerShell to Disable NBT-NS

9. Utilise non-standard port configurations for Remote Desktop Protocol (RDP) to minimise the attack surface. Video Demonstration
10. Physical security measures are also in place to protect servers housing domain controllers.
11. Finally, in the context of preventing the evolving social engineering attacks and phishing attempts, we conduct security awareness training for users to prevent social engineering attacks and phishing attempts.

VPN Setup

We have also enhanced our network security by implementing a VPN server. This strategic move allows us to establish a secure and private connection between our client PCs and our server. We ensure a seamless and protected communication channel by configuring VPN settings on the client PCs. This not only enhances the overall security of our network but also facilitates efficient data transfer, creating a reliable and robust infrastructure for our operations. Video Demonstration

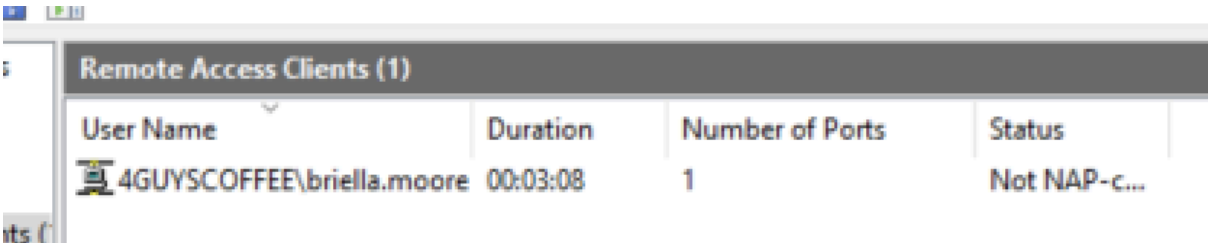
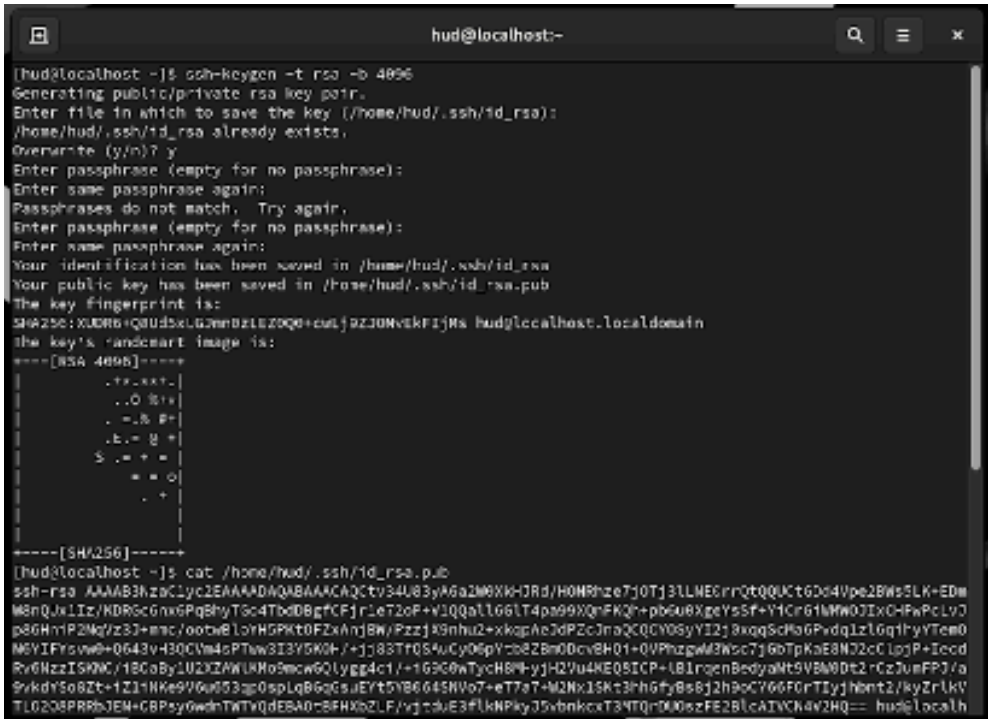
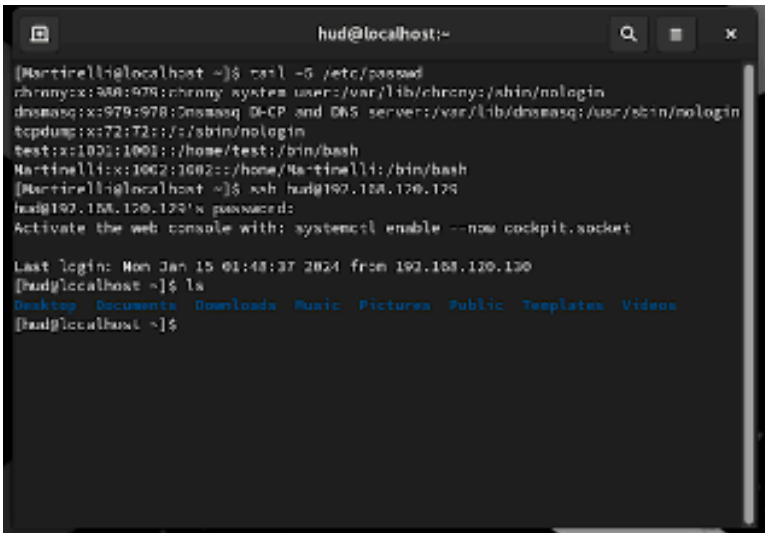
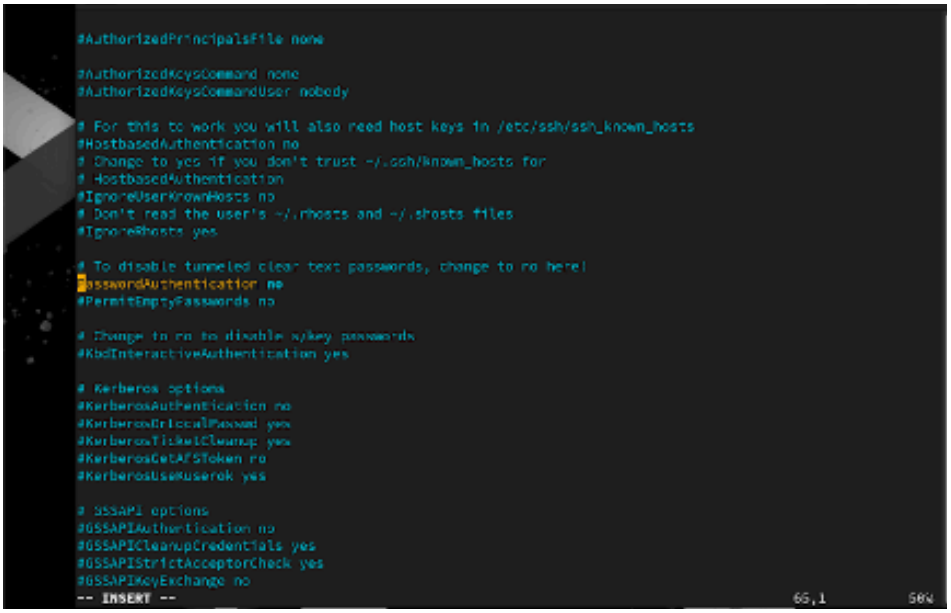


Figure 3.17: Successful VPN connection to the server

Hardening Web Server for Linux








```
[root@localhost Documents]# ls -l
total 12
drwxr-xr-x. 2 root root  42 Feb  5 06:31 app
-rwxr-xr-x. 1 hud  hud  252 Dec  6 20:59 coffee
-rw-r--r--. 1 hud  hud  352 Dec  6 20:59 newfile.txt
-rw-r--r--. 1 root root   0 Feb  5 01:36 rhel-9.oval.xml
-rwxr--r--. 1 hud  hud   36 Dec  7 20:47 script.sh
-rw-rw-rw-. 1 hud  hud    0 Dec  7 20:57 test2.txt
-rw-r--r--. 1 hud  hud    0 Dec  7 20:56 test.txt
[root@localhost Documents]# ls -l app
total 0
-rw-r--r--. 1 root root 0 Feb  5 01:34 index.html
-rw-r--r--. 1 root root 0 Feb  5 01:34 styles.css
[root@localhost Documents]# chmod +t app
[root@localhost Documents]# ls -l
total 12
drwxr-xr-t. 2 root root  42 Feb  5 06:31 app
-rwxr-xr-x. 1 hud  hud  252 Dec  6 20:59 coffee
-rw-r--r--. 1 hud  hud  352 Dec  6 20:59 newfile.txt
-rw-r--r--. 1 root root   0 Feb  5 01:36 rhel-9.oval.xml
-rwxr--r--. 1 hud  hud   36 Dec  7 20:47 script.sh
-rw-rw-rw-. 1 hud  hud    0 Dec  7 20:57 test2.txt
-rw-r--r--. 1 hud  hud    0 Dec  7 20:56 test.txt
[root@localhost Documents]# chmod g-x app
[root@localhost Documents]# ls -l
total 12
drwxr--r-t. 2 root root  42 Feb  5 06:31 app
-rwxr-xr-x. 1 hud  hud  252 Dec  6 20:59 coffee
-rw-r--r--. 1 hud  hud  352 Dec  6 20:59 newfile.txt
-rw-r--r--. 1 root root   0 Feb  5 01:36 rhel-9.oval.xml
-rwxr--r--. 1 hud  hud   36 Dec  7 20:47 script.sh
-rw-rw-rw-. 1 hud  hud    0 Dec  7 20:57 test2.txt
-rw-r--r--. 1 hud  hud    0 Dec  7 20:56 test.txt
[root@localhost Documents]#
```

Figure 3.18-3.21: Adding a sticky bit to the app directory containing web files to avoid deletion and giving only reading rights.

Securing a Linux server involves a series of fundamental steps to fortify its defences against potential threats and vulnerabilities. Keeping the system software and applications up-to-date is crucial by regularly applying security patches. Implementing strong password policies and ensuring that only necessary services are running help reduce the attack surface. Disabling unnecessary user accounts and employing multi-factor authentication further strengthens access controls.

Configuring firewalls, such as IPtables, to control incoming and outgoing traffic enhances network security. Restricting access through SSH keys rather than passwords adds an extra layer of protection. Regularly auditing and monitoring system logs provide insights into potential security incidents, enabling timely response and mitigation.

The benefits of hardening a Linux server are multifaceted. Enhanced security measures reduce the risk of unauthorised access, data breaches, and potential disruptions. Minimising unnecessary services and tightening access controls diminishes the attack surface, making it more challenging for malicious actors to exploit vulnerabilities. Regular system audits contribute to early threat detection and allow for proactive measures to maintain the integrity and reliability of the server. In essence, the hardening process is essential for safeguarding the server's overall stability and protecting sensitive information from potential cyber threats.

3. Secure Cloud Environment

AWS Solutions

1. Optimise Inventory and Sourcing:

Amazon DynamoDB: Manage inventory levels across all cafes and warehouses in real-time, facilitating efficient ordering and preventing stockouts.

- Highly scalable NoSQL database: Manage real-time inventory levels across all cafes and warehouses, even with many concurrent users.
- Flexible data model: Adapt the database schema to specific needs for storing diverse data like coffee bean varieties, roasting profiles, and customer orders.
- Fast and consistent performance: Ensure quick access to critical data for efficient order fulfilment and inventory management.
- Globally distributed: The database can be replicated across multiple regions for high availability and disaster recovery.

AWS IoT Core: Connect smart sensors in warehouses and roasting facilities to monitor conditions and ensure optimal bean storage and roasting.

- Connect smart devices: Manage sensors in cafes and warehouses to monitor temperature, humidity, and energy consumption for optimal bean storage and sustainable operations.
- Collect and analyse data: Gather real-time data from connected devices to optimise roasting processes, track bean usage, and predict demand.
- Remote monitoring and control: Manage equipment remotely and ensure consistent quality across various cafe locations.
- Scalable: Add or remove devices as needed without significant infrastructure changes.

Amazon Forecast: Predict coffee bean demand based on historical data and seasonal trends, reducing waste and optimising sourcing.

2. Enhance E-commerce Operations:

Amazon Elastic Compute Cloud (EC2): Scalable virtual servers to host the e-commerce platform with high availability and performance.

- Flexible compute resources: Host the e-commerce platform and website on virtual servers with customisable configurations.
- Scalability: Scale our computing power up or down based on traffic demands and business growth.
- High availability: Deploy the application across multiple servers for redundancy and prevent downtime.
- Familiar environment: Choose from various operating systems and software configurations to meet requirements.

Amazon Simple Storage Service (S3): Store product images and website content securely and reliably.

- Durable and scalable storage: Store website content, product images, roasted coffee bean photos, and customer data securely and reliably.
- Cost-effective: Pay only for the storage we use, making it efficient for various data types.

- Global accessibility: Access our data from anywhere globally with low latency.
- Disaster recovery: Backup our data automatically to protect against accidental loss or downtime.

Amazon CloudFront: Deliver website content and images faster to customers worldwide through a network of edge locations.

- Fast content delivery: Deliver website content and images to customers worldwide with low latency through a network of edge locations.
- Reduced bandwidth costs: Improve content delivery efficiency and minimise costs by caching frequently accessed data closer to customers.
- Improved user experience: Faster loading times for our website and e-commerce platform can boost customer engagement and conversions.
- Security: Secure our content against cyberattacks and malicious traffic with AWS security features.

Amazon Cognito: Securely manage customer accounts and orders with user authentication and authorisation features.
Amazon Pay: Provide a convenient and secure payment gateway for international customers.

3. Streamline Global Operations:
Amazon Virtual Private Cloud (VPC): Create a secure network for managing cafe operations and e-commerce activities across different countries.

- Secure infrastructure: Creates a private network for our cafe operations and e-commerce activities, ensuring data security across countries.
- Centralised control: Manage access and security policies for all resources within the VPC from a single location.
- Compliance: Helps meet data privacy regulations by isolating our data from the public internet.
- Flexibility: Customize our network setup to suit our needs and security requirements.

AWS Lambda: Automate processes like order fulfilment, inventory updates, and marketing campaigns based on triggers.

- Streamlines workflows: Automate inventory updates, order fulfilment, and email notifications without managing servers.
- Cost-effective: Pay only for the code execution time, ideal for sporadic tasks.
- Scalable: Handles peaks in demand effortlessly without provisioning additional servers.
- Integrations: Connect seamlessly with other AWS services like DynamoDB and S3 for a comprehensive workflow.

Amazon QuickSight: Gain data-driven insights from sales, customer behaviour, and operational metrics to make informed business decisions.
AWS Management Console: Centrally manage and monitor all AWS resources used by 4GuysCoffee from the Melbourne headquarters.

4. Build Brand and Engage Customers:

Amazon S3 Glacier: Store historical data backups and e-commerce images in a cost-effective archive storage solution.

- Long-term archive storage: Store historical data backups, website logs, and older e-commerce images in a cost-effective and secure archive storage solution.
- Reduced costs: Pay significantly less compared to standard S3 storage for data not frequently accessed.
- Data retrieval flexibility: Easily retrieve archived data when needed with convenient access management features.
- Scalability: Store massive amounts of historical data without worrying about space limitations.

Amazon SNS: Send targeted promotions and loyalty program updates to customers based on their purchase history and location.
Amazon Pinpoint: Personalize email marketing campaigns to drive customer engagement and sales.
Amazon Kendra: Develop a chatbot for our website to answer customer queries and provide product recommendations.

5. Ensure Sustainability and Security:

AWS Greengrass: Manage edge devices like smart sensors in cafes and warehouses efficiently for sustainable energy consumption.
AWS WAF: Secure our website and e-commerce platform from cyberattacks and malicious traffic.
AWS CloudTrail: Monitor and audit user activity across all AWS resources for enhanced security and compliance with data privacy regulations.

AWS Configurations

We meticulously set up key components to establish a robust and secure environment in configuring our AWS infrastructure. Our Virtual Private Cloud (VPC) was carefully designed, utilising specific subnets to compartmentalise different aspects of our operations. We implemented Network Access Control Lists (ACLs) to control inbound and outbound traffic at the subnet level, enhancing security. Additionally, we incorporated an Internet Gateway (IGW) to facilitate communication between our VPC and the broader internet, ensuring seamless connectivity. Within the VPC, we deployed an EC2 instance as our web server, leveraging Amazon's compute capabilities. Simultaneously, we configured an Amazon S3 bucket to securely store and manage our web content. This comprehensive setup aligns with our organisational needs, emphasising scalability, security, and efficient data management.

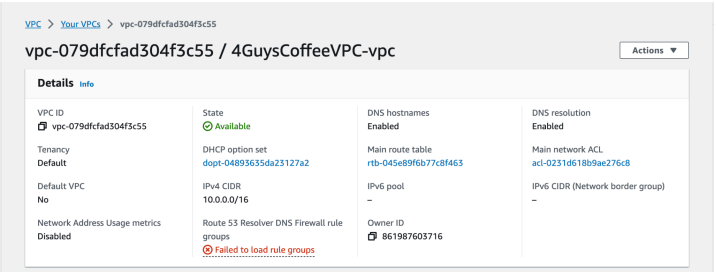


Figure 4.1: AWS settings for VPC configuration

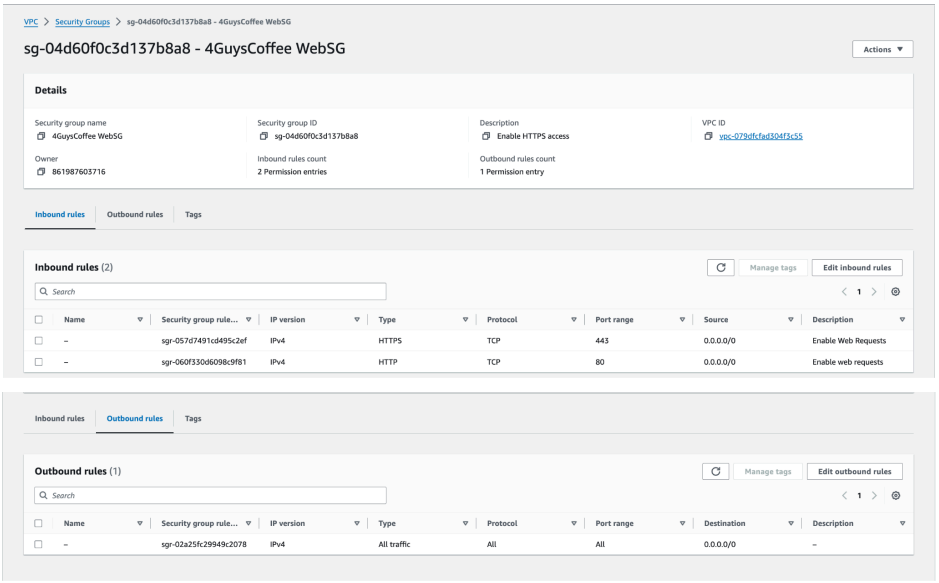


Figure 4.2: AWS VPC Inbound and Outbound rules

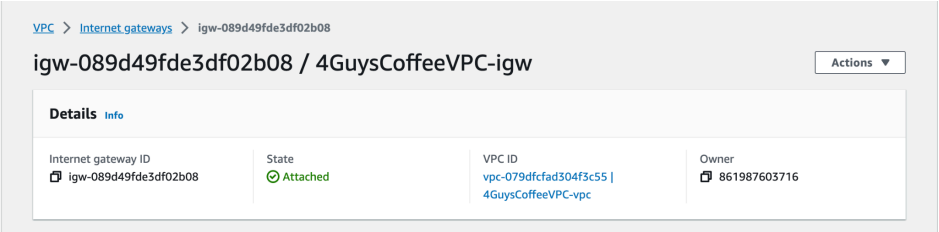
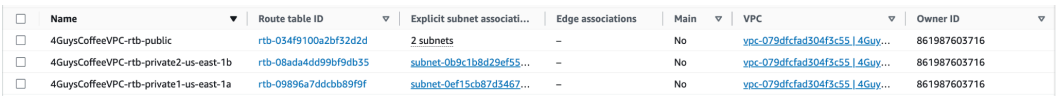


Figure 4.3: AWS IGW configuration



Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC	Owner ID
4GuysCoffeeVPC-rtb-public	rtb-034f9100a2bf32d2d	2 subnets	–	No	vpc-079dfcfad304f3c55 | 4Guy...	861987603716
4GuysCoffeeVPC-rtb-private2-us-east-1b	rtb-08ada4dd99bf9db35	subnet-0b9c1b8d29ef55...	–	No	vpc-079dfcfad304f3c55 | 4Guy...	861987603716
4GuysCoffeeVPC-rtb-private1-us-east-1a	rtb-09896a7ddcbb89f9f	subnet-0ef15cb87d3467...	–	No	vpc-079dfcfad304f3c55 | 4Guy...	861987603716

Figure 4.4: AWS Subnetting

Inbound			
Rule	**Type**	**Source**	**Allow / Deny**
99	HTTP	0.0.0.0/0	Allow
100	HTTPS	0.0.0.0/0	Allow
200	SSH	*System ADMIN*	Allow
300	Database	*Database IP*	Allow

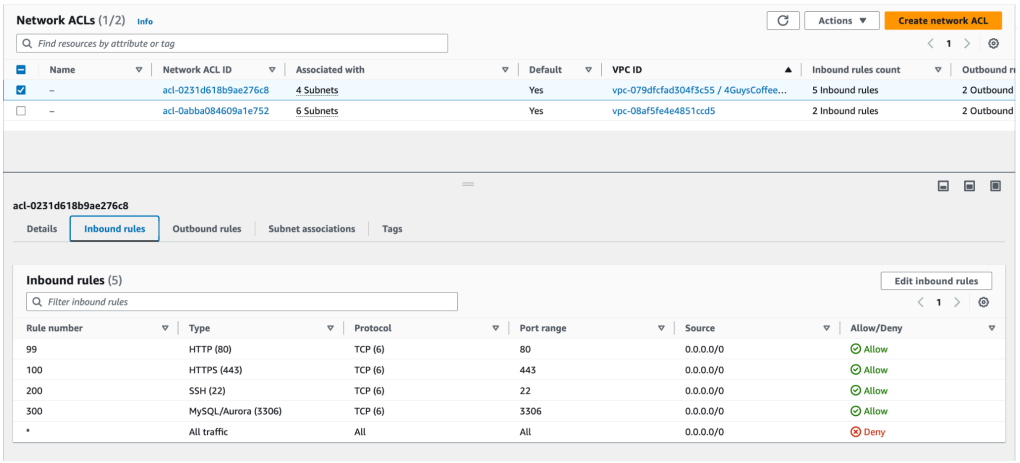


Figure 4.5: AWS Network ACL configurations

Outbound			
Rule	**Type**	**Source**	**Allow / Deny**
100	All Traffic	0.0.0.0/0	Allow

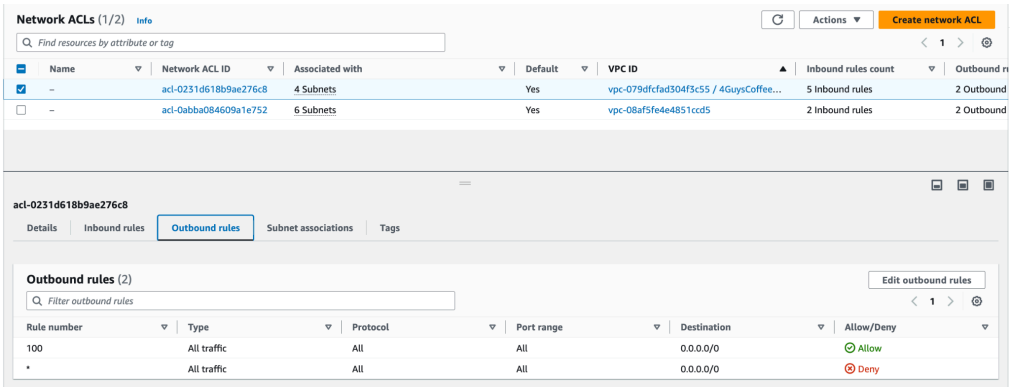


Figure 4.6: AWS ACL Outbound Rules

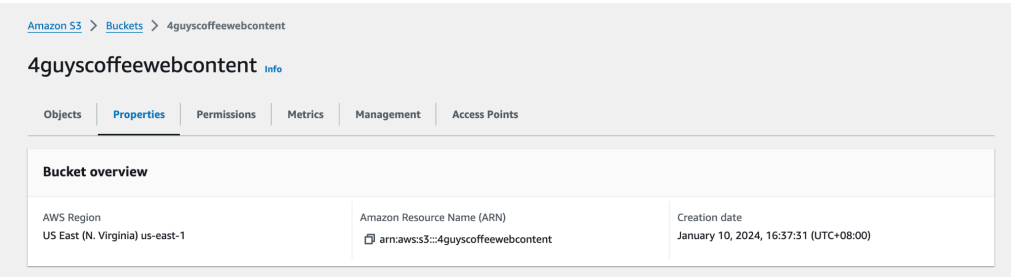


Figure 4.7: AWS S3 Configurations

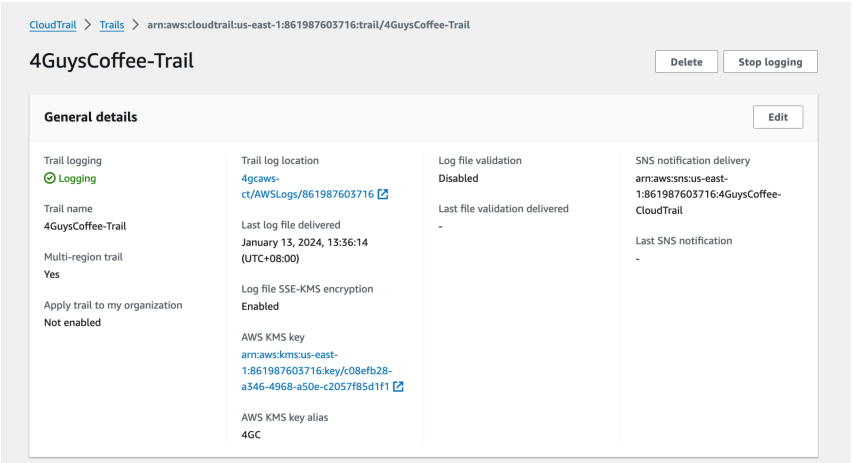


Figure 4.8: AWS CloudTrail Configurations

Implementing AWS CloudTrail for 4GuysCoffee is a strategic move that aligns with our commitment to transparency, security, and operational excellence. With CloudTrail, we gain unparalleled visibility into every interaction within our AWS infrastructure. This means we can monitor and audit changes made to our resources, ensuring that our AWS environment is secure and compliant. The detailed logs, stored securely in dedicated S3 buckets, are crucial for forensic analysis and compliance reporting. CloudTrail's ability to track data events, especially in our S3 storage, enhances our understanding of resource access and modification, offering valuable insights for continuous improvement.

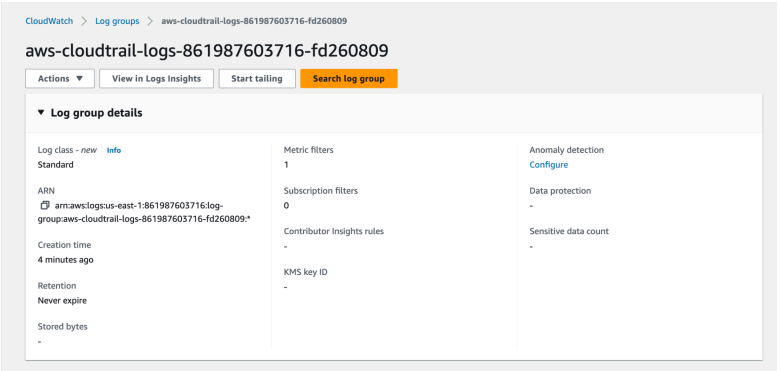


Figure 4.9: AWS CloudWatch Configurations

AWS CloudWatch emerges as a vital tool in our quest for real-time monitoring and actionable insights. By creating custom dashboards, we consolidate key metrics from various AWS resources, giving us a holistic view of our operational landscape. Alarms set in CloudWatch allow us to respond promptly to deviations from normal operating conditions. This means proactive issue resolution and improved overall system reliability. CloudWatch Logs centralises our log management, simplifying debugging and performance monitoring for our applications. Creating custom metrics ensures a tailored understanding of our application's performance, empowering us to optimise user experiences across our cafes and e-commerce platforms.

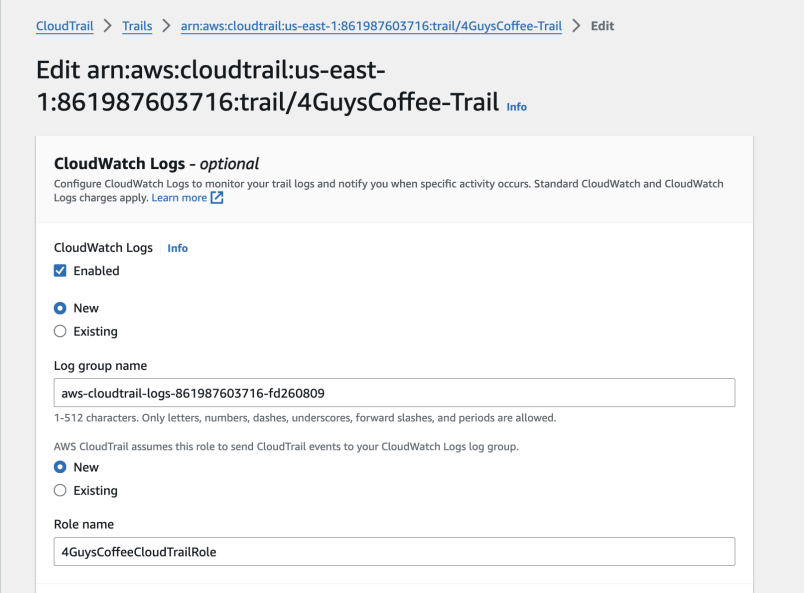


Figure 4.10: AWS CloudTrail & CloudWatch Integration

The integration of AWS CloudTrail, CloudWatch, and Simple Notification Service (SNS) stands as a pivotal enhancement for 4GuysCoffee, offering a holistic approach to monitoring and managing our AWS infrastructure. With CloudTrail, we gain a meticulous audit trail of every interaction, ensuring transparency and bolstering our commitment to security and compliance. The seamless integration with CloudWatch allows us real-time visibility into our operational landscape through custom dashboards, empowering us to address issues and optimise system reliability proactively. CloudWatch Alarms, integrated with SNS, provide instant notifications, ensuring that our team stays informed about critical events, from security breaches to operational anomalies. This trifecta of services fortifies our ability to maintain the integrity of our AWS environment and streamline communication, enabling swift responses to potential challenges. As a result, our commitment to a secure, efficient, and customer-focused operation in the global coffee industry is further solidified, ensuring that we stay ahead in this dynamic and competitive market.

4GuysCoffee harnesses a robust set of AWS services to optimise its operations comprehensively. Amazon DynamoDB facilitates real-time inventory management across

cafes and warehouses with its scalable NoSQL database, while AWS IoT Core connects smart sensors for efficient monitoring and control. Amazon EC2 ensures a scalable and highly available hosting environment for the e-commerce platform, supported by Amazon S3 for secure storage of product images and content. The global reach is enhanced through Amazon CloudFront, providing faster content delivery. Streamlining global operations is achieved with Amazon VPC, and AWS Lambda facilitates automation. In pursuing sustainability and security, AWS Greengrass manages energy consumption, and AWS WAF and AWS CloudTrail ensure robust cybersecurity measures. These services empower 4GuysCoffee to thrive in a dynamic, secure digital landscape while delivering an enhanced customer experience.

4. Cybersecurity Fundamentals

Background and Scope

Amidst our success in the coffee industry, 4GuysCoffee recognises the lurking potential for cyberattacks. As we have expanded into e-commerce, the online platform selling our products presents new vulnerabilities, particularly to digital skimming and its ilk. To fortify our defences, we are committed to a holistic cybersecurity approach.

This approach, encompassing employee training, continuous security assessments, robust encryption, and expert collaboration, aims to build resilience against evolving digital threats. This proactive report stems from our unwavering dedication to protecting 4GuysCoffee's digital assets. Herein, we will dissect the tactics of common cybercrimes along with a couple of case studies, expose potential weaknesses in our system, and lay out concrete steps to avoid pitfalls like digital skimming. By embracing these preventative measures, we safeguard not only our digital storefront but also the trust and security of our cherished customers. This report serves as a blueprint for achieving this critical objective.

Attack Vector Landscape

Digital Skimming

Visa's Biannual Threats Report of 2022 identified Digital Skimming as one of the upcoming Cybersecurity threats. Digital Skimming attacks involve cybercriminals injecting malicious code onto a merchant's website, primarily focusing on checkout pages to harvest payment account details and customers' personally identifiable information. These attacks often exploit misconfigurations or insufficient security controls in a merchant's environment, allowing threat actors to deploy the malicious skimming code successfully.

Digital skimming, also known as Magecart attacks, involves the covert insertion of malicious code into the payment processing pages of websites. This malicious code is designed to capture sensitive customer information, such as credit card details, during the online checkout process.

Impacts & Consequences

As reported by Visa in 2022, its Payment Fraud Disruption (PFD) team identified an evolution to the pre-existing modus operandi. Threat actors can now place "a reverse shell dropper on the targeted eCommerce merchant's file system. Once a shell session has been initiated, the reverse shell (or 'connect-back shell') redirects the input and output connections of the victim's system, allowing the attacker remote control over the system. Once the attacker gains control over the victim's system, they append malicious digital skimming JavaScript code into the legitimate code of the victim's eCommerce platform's checkout webpage. This malicious digital skimming code harvested payment account data as victims entered the data into the site's checkout fields. The malware harvested the victims' full PAN, expiration date, and cardholder information".

The consequences of a successful digital skimming attack can be far-reaching and devastating. They extend beyond financial losses, as they can erode customer trust and damage the reputation of our beloved brand.

For individuals, the primary concern is the theft of sensitive financial information, including credit card numbers, expiration dates, and CVVs. This could result in unauthorised charges, fraudulent transactions, and financial hardship for victims. Moreover, stolen payment card data can be used for identity theft, where criminals take on the victim's financial identity to open new accounts, obtain loans, or commit other fraudulent activities. This can significantly damage the victim's credit score and cause long-term financial problems.

On the other hand, affected businesses could be hit with hefty fines and legal repercussions from regular payment card processors. Most notably, investigating and mitigating a skimming attack can be time-consuming and resource-intensive, disrupting business operations and potentially leading to revenue loss.

Trend Analysis

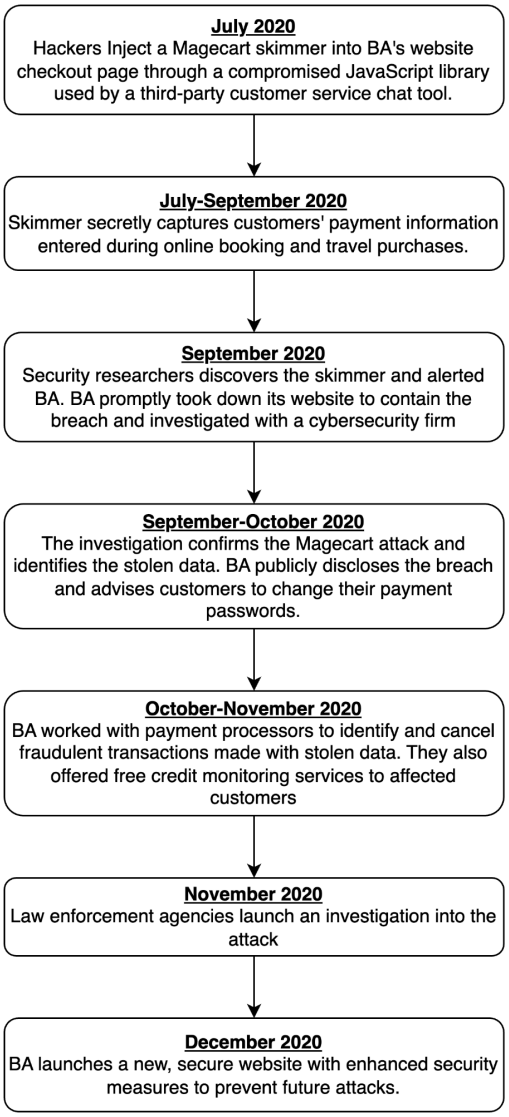
According to Allied Market Research, the projected Compound Annual Growth Rate (CAGR) for the digital payment market will be 17.2% by 2032.
The market is experiencing significant growth driven by the widespread adoption of digital payments in online shopping. This surge is primarily attributed to time efficiency and convenience. Additionally, the market is propelled forward by the advent and ubiquity of smartphones, fast internet connectivity, a growing consumer preference for digital payments, and widespread acceptance of this payment method among merchants.
This increases the number of users exposed to e-skimming threats and contributes to their evolution. Unlike conventional methods, e-skimming attacks persistently intercept customer payment details during the point of purchase, making them challenging to identify and often invisible to both customers and retailers. Most e-skimming incidents are only detected after weeks or even months of operation. The mean time to detect (MTTD) and mean time to respond (MTTR) for client-side security breaches are incredibly long. Attackers have also integrated valid SSL certificates linked to domains delivering malicious code, creating the illusion of legitimate traffic and preventing customers from receiving mixed content warnings when the website blends trusted, encrypted content with unencrypted malicious content.

A recent report has detailed Magecart attacks in which misconfigured access controls on Amazon S3 buckets enabled attackers to append their skimmer code to existing JavaScript application code files. This was made even easier with automated AWS S3 scanners that they have developed that enable them to detect misconfigured S3 buckets.
As explored earlier, Magecart operators are well-known for their capacity to adjust and refine their strategies. In recent years, they have utilised 404 error pages – a standard feature on every website– to conceal and execute their malicious code designed for stealing credit card information. This method is a novel utilisation of the default '404 Not Found' page, which distinguishes it. As described by Akamai Security Intelligence in their report, “This concealment technique is highly innovative and something we have not seen in previous Magecart campaigns.”

Case Study: British Airways Magecart Attack

During the summer of 2020, British Airways (BA) experienced a sophisticated Magecart attack. Cybercriminals implanted malicious code into the airline's website, targeting the checkout page for online bookings and travel transactions. This code surreptitiously collected sensitive customer payment details, such as credit card numbers and CVVs.

The breach remained undetected for months, potentially affecting many travellers. Fortunately, upon discovery, BA promptly responded by shutting down the compromised website, investigating the breach, and informing affected customers. They worked diligently to contain the fallout by cooperating with payment processors to identify and nullify fraudulent transactions. Additionally, BA offered credit monitoring services to individuals affected by the incident. Here is a breakdown of the attack timeline:



Despite the swift response to the breach, it is undeniable that customer data was compromised, leading to significant repercussions for British Airways under GDPR. Initially facing a fine of £183 million, the penalty was later reduced to £20 million. This incident underscores the peril digital skimming attacks pose to businesses.

How Magecart Attacks Could Brew for 4GuysCoffee

As the aroma of freshly roasted coffee beans fills our office, a chilling fact simmers beneath the surface – the potential for a Magecart attack to disrupt our cherished 4GuysCoffee experience. Just as British Airways faced a brutal data skimming attack, our login and checkout pages could become invisible honey traps, silently syphoning customer data, leaving a bitter aftertaste of fear and distrust.

The spectre of Magecart lurks in the shadows of compromised plugins or third-party scripts, injecting malicious code into our online haven. This digital gremlin, unseen by our customers, intercepts entered information – credit card numbers, CVVs, login credentials – brewing a potent storm of financial and reputational damage. The consequences stretch far beyond stolen data, with potential lawsuits, fines, and a tarnished brand image threatening to engulf our carefully crafted cup of comfort.

Suggested Controls & Mitigation

At 4GuysCoffee, security is not an afterthought but the secret ingredient that keeps our virtual cup brimming with customer satisfaction. The rise of online skimming attacks serves as a cautionary signal for service providers and merchants. Magecart hackers are getting increasingly creative in developing JavaScript sniffers capable of compromising any e-commerce site lacking adequate security measures. Consequently, proactive steps must be taken to address this growing threat.

We recommend these industry-practised preventive measures:

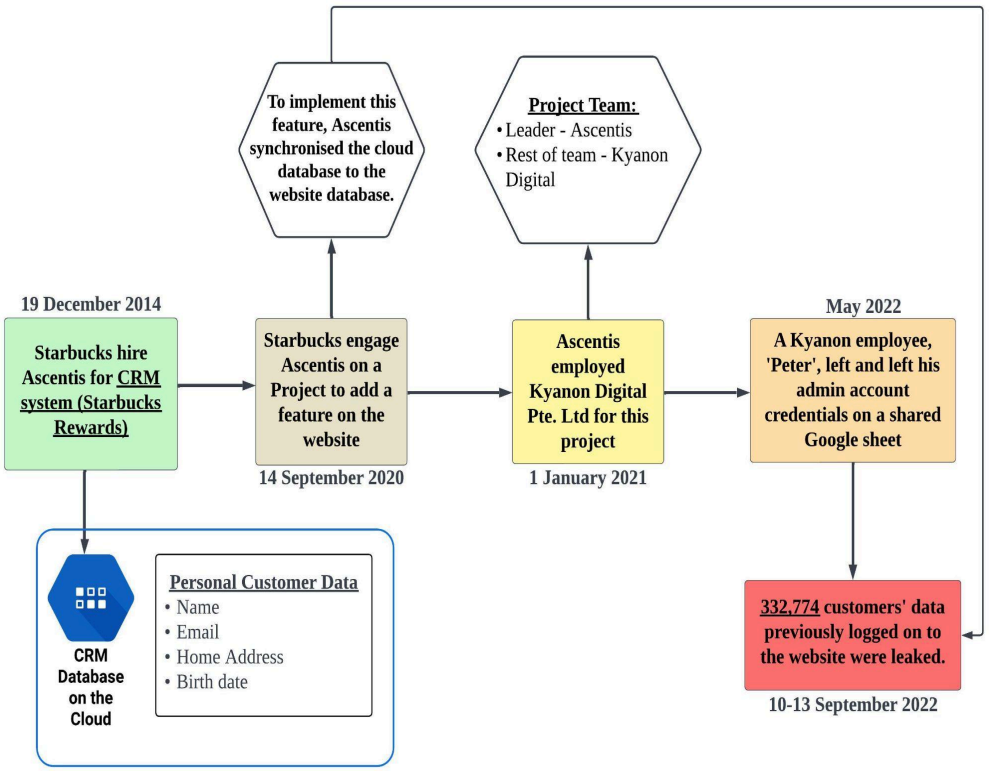
1. Regularly inspect the code for vulnerabilities.
2. Update login credentials regularly.
3. Given that the recent attacks exploit misconfigured write permissions in widely-used CDNs such as our AWS resources, it is imperative to appropriately configure and limit secure access to these resources and the overall CDN implementations.
4. Employ a unified and secure configuration for all implementations to avoid inconsistencies.
5. Implement Web Application Firewalls (WAFs) to help block malicious code injections.
6. Implement proactive measures such as penetration testing to uncover vulnerabilities, timely patching to address gaps, and maintaining multi-layered security systems to thwart intrusions.

For enhanced security, merchants and service providers are strongly advised to utilise solutions management systems such as the Security Information and Event Management (SIEM). “Check-out Solutions” are also instrumental in these situations as they enable customers to input transaction information on a separate payment page, redirecting them away from the primary e-commerce site.

Starbucks Singapore Data Breach

In September 2022, around 330,000 Starbucks customers' data were leaked and put up for sale on an online forum. The coffee chain was only made aware of this leak three days later, and the affected customers were notified via email almost a week later. The affected customers had accounts and made online transactions on the website or the mobile application. The PDPA Act was violated. Information on the case was based on the report released by the Personal Data Protection Commission in 2023.

Overview of the Data Breach



On December 19, 2014, Starbucks SG enlisted the Organization's expertise to develop, implement, support, and host a Customer Relationship Management system called the "CRM System." This system was crucial in supporting Starbucks SG's "My Starbucks Rewards" loyalty program, with the Organization responsible for its overall management.

Upon joining the Rewards Program, individuals would provide their details, such as name, email address, telephone number, and birth date. These details were meticulously collected and stored in the "CRM Database."

Fast forward to September 14, 2020, Starbucks SG reached out to Ascentis Pte. Ltd. through their website for the sale and purchase of Starbucks SG products. This marked the beginning of a collaborative effort, leading to Ascentis Pte. Ltd. engaging the services of Vietnamese tech organisation Kyanon Digital on January 1, 2021. Kyanon Digital's role was to provide additional manpower and software development support for the ongoing project.

A notable feature and project requirement involved auto-completing members' data when filling out forms on the website. Consequently, this led to the creation of an additional copy of the customer database, hosted and operated independently from the original cloud database, on the website platform.

While Ascentis Pte. Ltd. was in control and managed the project, the actual implementation was carried out by Kyanon Digital employees. These employees held accounts with administrator privileges for the website platform, including the ability to export data from it.

In May 2022, a pivotal moment occurred when one of the employees, 'Peter,' left the company. Unfortunately, he also left his admin account credentials on a shared Google sheet. To complicate matters, his account remained active, and despite a password change to 'Kyanon@123456,' other employees continued using the account.

Between September 10 and 13, a malicious actor exploited Peter's admin account, granting admin access to other accounts, gathering data, and exporting it to an external email address. The repercussions were significant, with 332,774 individuals falling victim to the breach. This included sensitive information such as names, email addresses, dates of birth, physical addresses of 181,875 individuals, and telephone numbers of 310,560 individuals.

The aftermath saw the compromised data being auctioned on a dark web forum. Prompt action was taken, with the Singapore Computer Emergency Response Team being notified on September 13, 2022. Starbucks SG and Ascentis Pte. Ltd. swiftly submitted data breach notifications to SGPDPC on September 15 and 16, 2022, respectively.

Attack Vectors

- Account Takeover - It was reported that the admin accounts only had single-factor authentication. Moreover, the login credentials passed on were not encrypted and shared with the entire project team on a Google document. Also, when the password was changed, although it met the requirements, it was predictable and included the company’s name, making it more susceptible to attack.
- Distributed Data Storage - The data was replicated and stored in a database on the website, which was hosted and operated independently. This increases the attack surface significantly.
- Lack of Access Management - Admin privileges were granted to all team members; hence, every team member had full access to the data and could modify it, export it, etc. An issue of roles
- Lack of encryption - The data stored on the platform's web server was not encrypted.
- Lack of Detection Measures - Ascentis Pte. Ltd. did not pick up on the data breach and incident until the SGCERT team was notified of the data being sold and auctioned on the dark web. No checks or alerts were raised, especially when an email was sent to an external email address, and other accounts were granted admin privileges.

- Lack of Security Policies - No proper exit clearance and procedures were enforced for ‘Peter’ with his account (with admin privileges) not being disabled after he resigned from the company.

Solutions

The case study above of Starbucks SG’s customer data breach is highly applicable and relevant to our coffee business, which has an online store and a member system. By analysing the case study and identifying the vulnerabilities that have been or could have been exploited by malicious threat actors, we have devised the following solutions to mitigate the risks involved.

The fortification of information security within the organisational framework is paramount, necessitating the formulating of a comprehensive security policy. This strategic approach seeks to generalise the attack surface and ensure adherence to prevailing laws and regulations. Critical measures encompass the mandatory implementation of Multi-Factor Authentication (MFA) for administrator accounts, validating access authenticity. Stringent password hygiene protocols are advocated to enhance security, mandating the creation of passwords devoid of corporate relevance. The operationalisation of the principle of least privilege is proposed, facilitated by the delineation of roles and responsibilities by the project lead, ensuring judicious allocation of access rights. To bolster organisational security, the institution of a systematic exit clearance and procedure is recommended, and accounts for departing personnel should be disabled promptly. A robust detection system is imperative to surveil and identify anomalous activities, minimising vulnerability to zero-day attacks. A unified database system is advocated for reduced attack surface and streamlined transaction management, while distributed databases require stringent authentication, authorisation, and data encryption. Routine data audits are prescribed for continuous IT infrastructure review, identifying and rectifying vulnerabilities in an ongoing commitment to robust security measures.

5. Ethical Hacking and Pentesting

Attack Description

The attacker, a competitor of 4GuysCoffee, initiates a comprehensive reconnaissance and enumeration process employing various tools such as Nmap, Recon-ng, and Netcraft to probe vulnerabilities within the company's infrastructure. Identifying a vulnerability in 4GuysCoffee's website through SQL injection, the attacker exploits this flaw, executing SQL commands to extract sensitive data from the 'user' table, which houses customer and staff credentials, including email addresses, names, and passwords.
With the acquired credentials, the attacker proceeds to log in to a customer's email account, facilitating the launch of a phishing attack on unsuspecting staff members, masquerading as a legitimate customer. Subsequently, leveraging sophisticated tools, the attacker attaches a backdoor to a seemingly innocuous PDF file, employing the compromised email account to distribute it to staff members. As the recipient fails to detect any suspicious elements within the PDF or its sender, assuming legitimacy due to the sender's verified customer status, the backdoor is unwittingly installed upon downloading the file.
This backdoor, operating as a reverse TCP connection, grants the attacker unhindered access to the company's network. Configuring a listener on the attacker's system facilitates remote access to the victim's machine, enabling the attacker to execute privilege escalation and infiltrate the company's file servers. Subsequently, critical files and folders of 4GuysCoffee are maliciously deleted, causing significant disruption to operations.
To conceal the attack, the attacker meticulously eradicates all traces of the installed backdoor and takes measures to cover their tracks, obfuscating any evidence linking them to the malicious activities.
Following the discovery of missing and deleted crucial information, the staff initiates an investigation into the incident, prompting the involvement of a forensic team tasked with uncovering the root cause of the breach and mitigating its impacts.

Recon and Scanning

The attacker conducted preliminary information gathering on 4guyscoffee.

Google
Using advanced search operators, hackers can locate the website for 4guyscoffee that would not appear in an ordinary Google search of ‘4guyscoffee’.

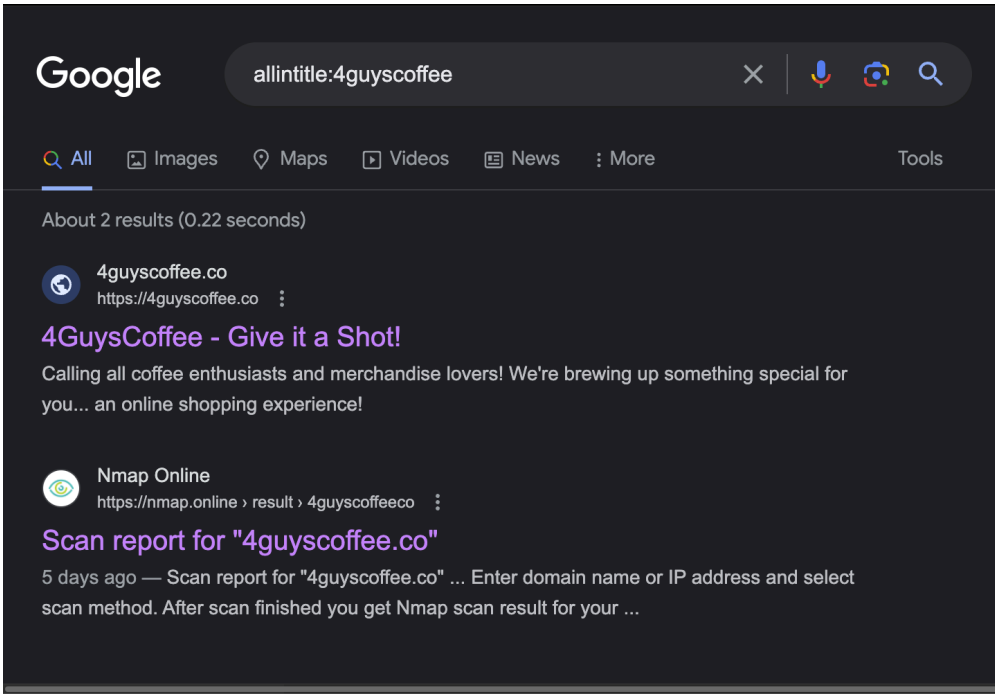
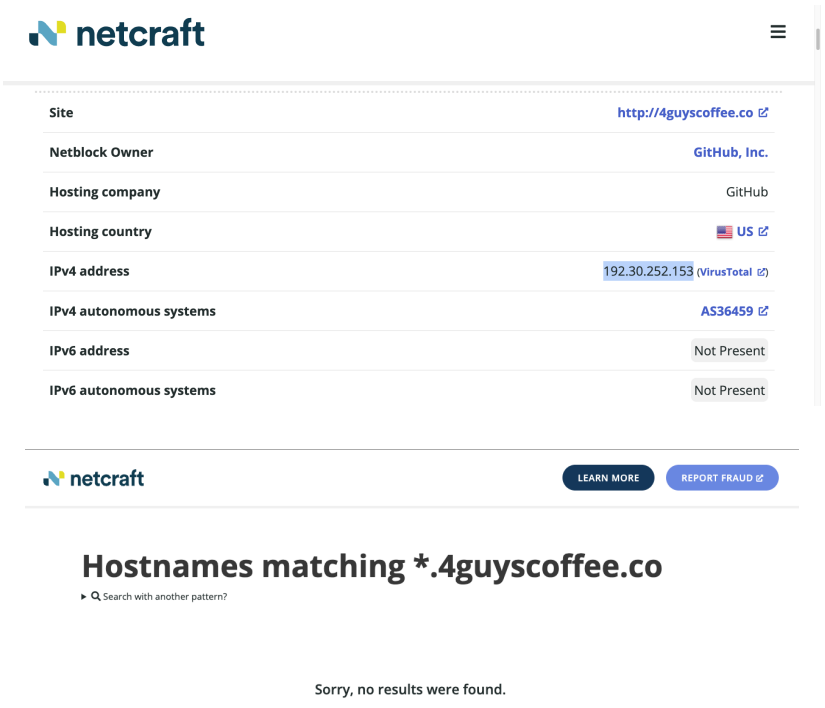
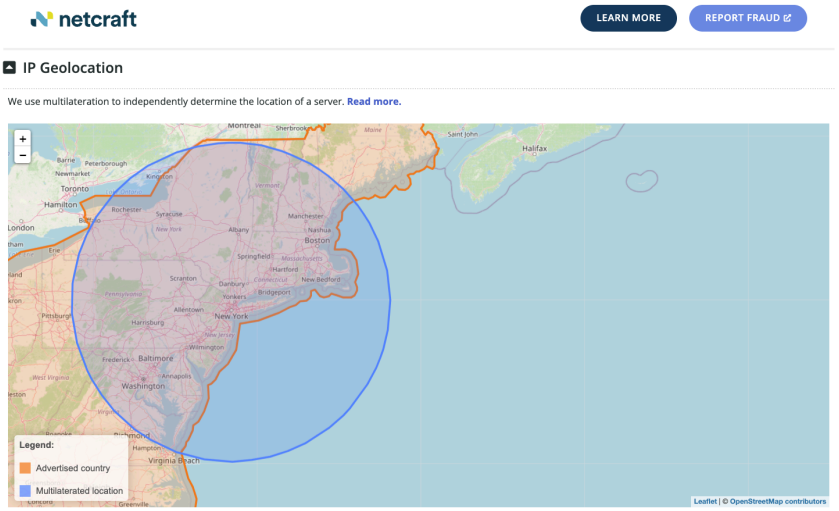


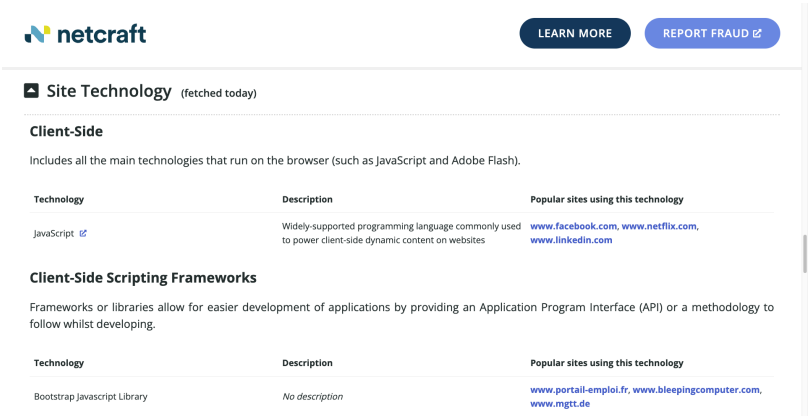
Figure 6.1: Google advanced search

Netcraft

Knowing the URL, an attacker would use Netcraft to obtain information on the website's IP address, if any other subdomains are present, and information on the hosting system. Information such as the technology stack of the website is also displayed.







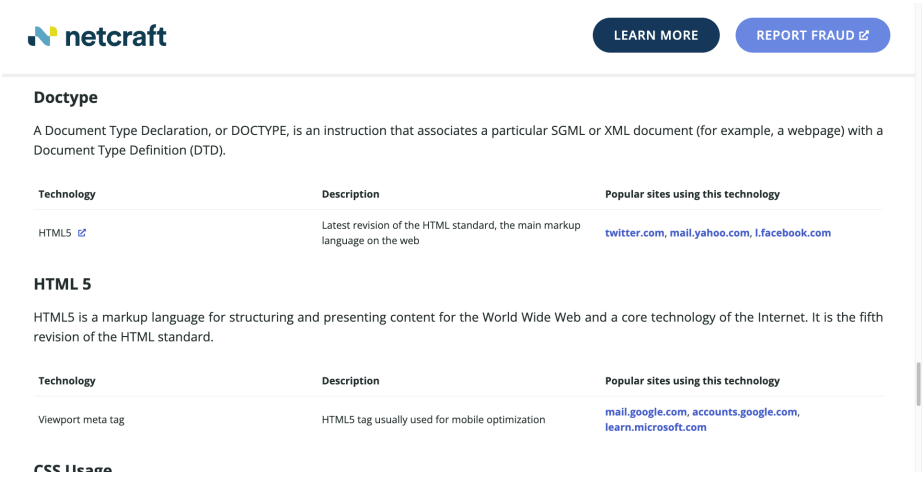


Figure 6.2 - 6.6: Netcraft scan results

As an attacker, we aim to infiltrate the network and website of our target, 4GuysCoffee.co, using penetration testing tools to uncover vulnerabilities ripe for exploitation. Leveraging tools like Nmap and Nessus, we conducted thorough port scans and vulnerability assessments to identify entry points and weaknesses in the network infrastructure. Once potential vulnerabilities were pinpointed, we focused on the website, employing web

vulnerability scanners such as OWASP ZAP and Burp Suite to crawl through the site's pages and uncover flaws like SQL injection and cross-site scripting.

Armed with this valuable reconnaissance, we craft targeted attacks to exploit the identified vulnerabilities, gain unauthorised access to systems, and compromise sensitive data. Our ultimate goal is to breach the network defences and compromise the integrity and security of 4GuysCoffee's digital assets. Through meticulous testing and exploitation, we seek to uncover weaknesses that could be exploited by malicious actors and highlight the importance of robust cybersecurity defences in safeguarding against such threats.

Network Scanning Tools:

- Nmap
- Nessus
- OpenVAS
- Wireshark
- Angry IP Scanner
- Zenmap
- Netcat

Website Scanning Tools:

- OWASP ZAP (Zed Attack Proxy)
- Burp Suite
- Nikto
- Netsparker
- Arachni
- Grabber
- Wapiti

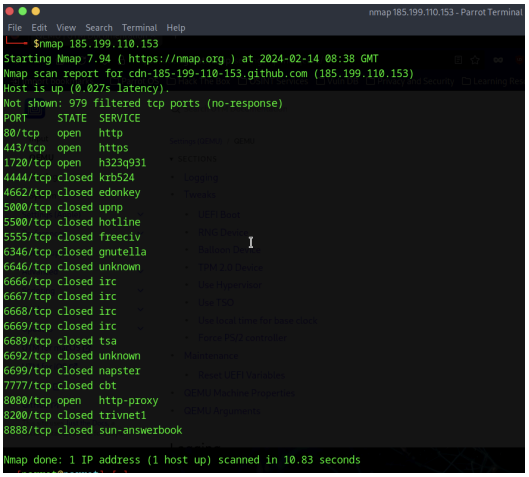


Figure 6.7: NMAP scan of 185.199.110.153 (http://4guyscoffee.co)

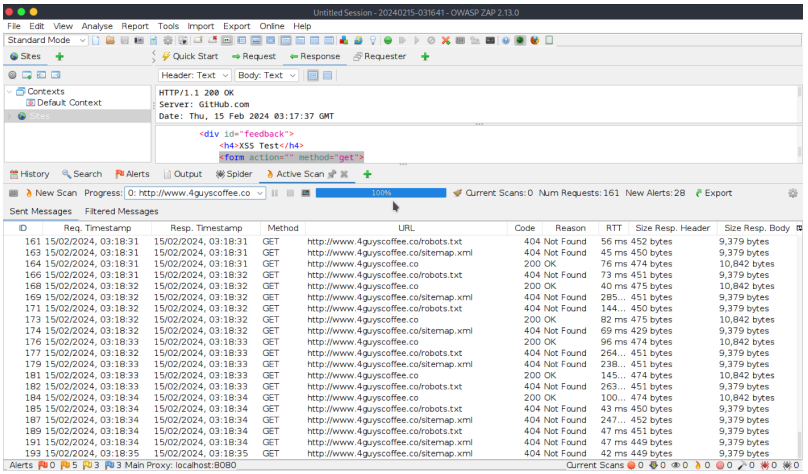


Figure 6.8: OWASP ZAP scan of http://4guyscoffee.co

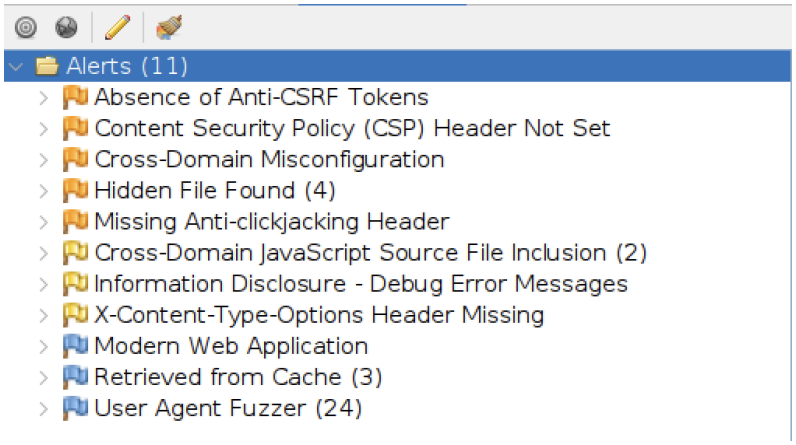


Figure 6.9: Vulnerabilities on http://4guyscoffee.co

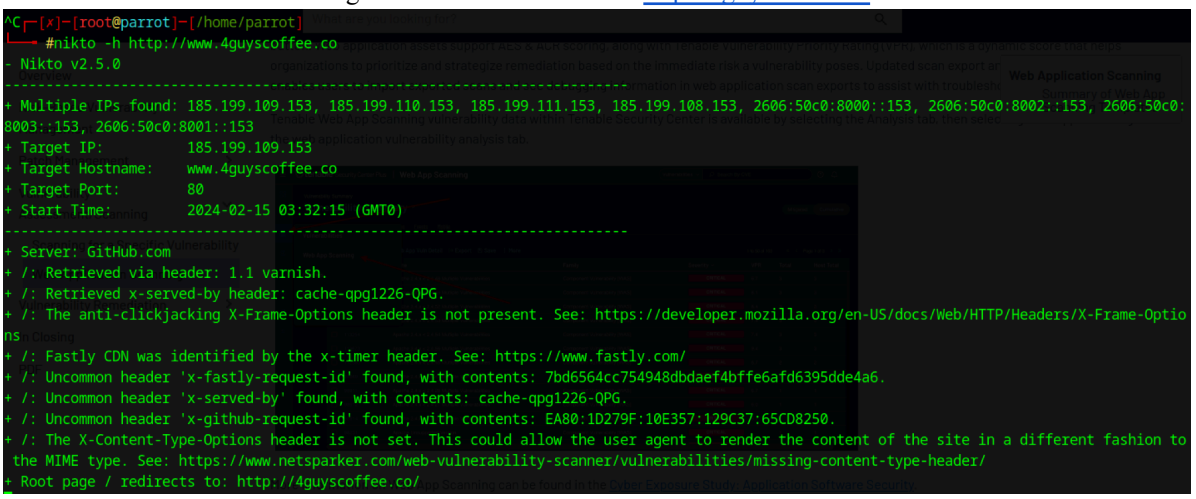


Figure 6.10: Nikto Scan on http://4guyscoffee.co

Attack

SQL Injection

The attacker, a threat actor attempting to exploit SQL injection vulnerabilities within 4GuysCoffee's website, systematically tested various SQL commands. Through this process, he encountered different error messages at different attack stages. These errors, ranging from generic error responses to more specific database-related errors, indicate the website's vulnerability to SQL injection. The varied responses confirm that the website is susceptible to manipulation through SQL injection attacks. Each error he encountered is a breadcrumb, guiding him towards potential entry points into the website's database. Armed with this knowledge, he recognises that persistently probing the website with diverse SQL injection payloads increases the likelihood of successfully breaching its defences and gaining unauthorised access to sensitive data or compromising its functionality.

Fatal error: Uncaught mysqli_sql_exception: Table 'test.users' doesn't exist in /Applications/XAMPP/xamppfiles/htdocs/login.php:17 Stack trace: #0 /Applications/XAMPP/xamppfiles/htdocs/login.php(17): mysqli->query('SELECT * FROM u...') #1 {main} thrown in **/Applications/XAMPP/xamppfiles/htdocs/login.php** on line **17**

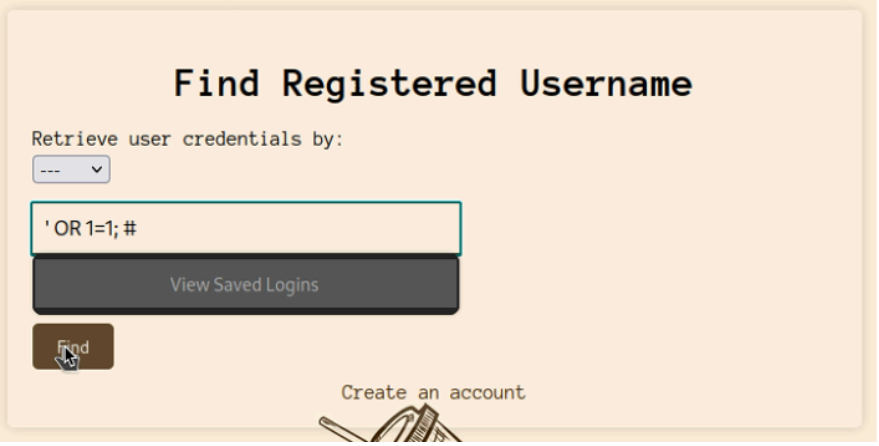


Figure 6.11 - 6.12: Attacker trying different SQLi techniques

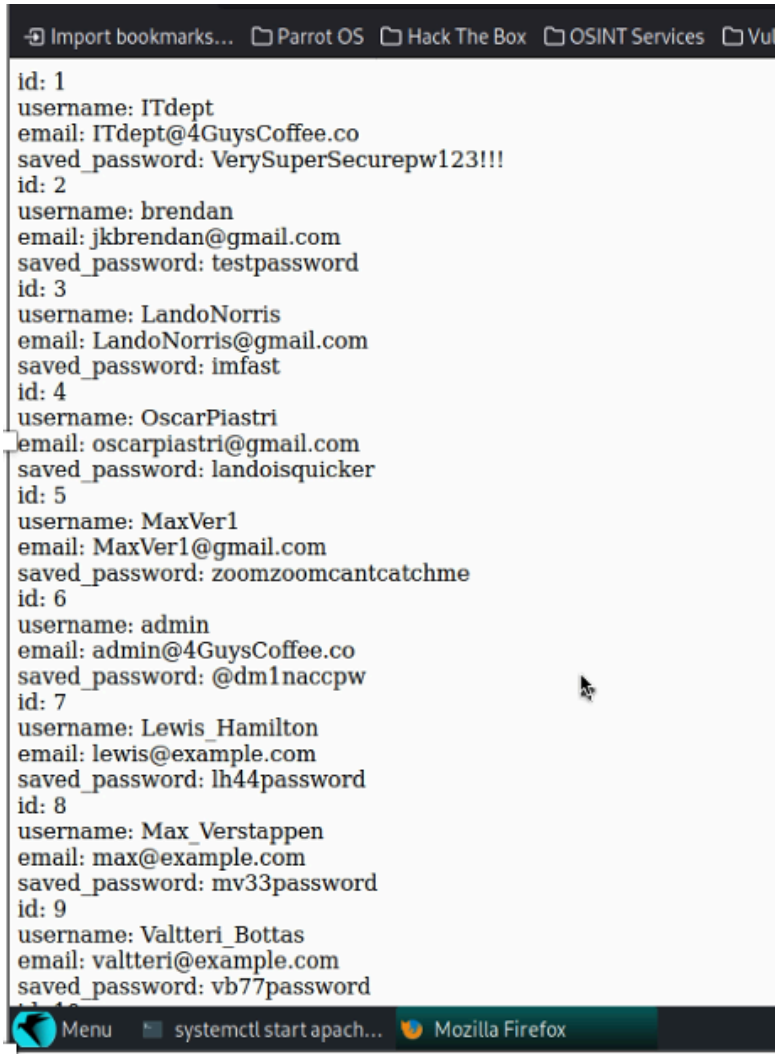


Figure 6.13: Attacker gains access on database

With this information, attackers are poised to execute a second stage of attack. Malicious actors intend to launch phishing campaigns targeting cafe staff by leveraging the extracted sensitive data. By utilising stolen customer information, the attacker will pose as one of the customers and trick staff members into downloading the PDF menu with a hidden backdoor. This backdoor presents a stealthy entry point, granting attackers unauthorised access to staff machines. Once infiltrated, the backdoor provides attackers with remote control over that compromised staff's machine, giving it access to and potentially compromising the security and privacy of customers and employees.

Reverse Shell Attack

Intending to breach the company's network and extract confidential information, the attacker employs sophisticated tactics. Leveraging the capabilities of Metasploit, they intricately embed a reverse shell into a seemingly innocuous PDF menu obtained from the company's website. This covertly inserted payload is a gateway for remote access to the victim's machine.

Utilising Meterpreter, a powerful post-exploitation tool within the Metasploit framework, the attacker establishes a listener, meticulously configuring it to await connections from the compromised system. This strategic setup enables them to remotely manipulate the victim's machine upon successfully executing the malicious PDF file.

Understanding the prevalence of password reuse among internet users, the attacker strategically sifts through the acquired user data, expecting to uncover individuals who exhibit this risky behaviour. They anticipate identifying at least four users with identical passwords across their 4guyscoffee accounts and other online platforms.

Systematically, the attacker initiates login attempts using the compromised email addresses, systematically probing for weaknesses in authentication protocols. After persistent efforts, they uncovered an account that not only shares the same password across multiple platforms but also lacks the additional security layer provided by Multi-Factor Authentication (MFA).

Capitalising on this vulnerability, the attacker crafts a meticulously designed phishing email aimed at the administrative staff of 4GuysCoffee. With a tailored message and an attachment masquerading as a legitimate document, the email aims to deceive the recipient into unwittingly executing the malicious PDF file.

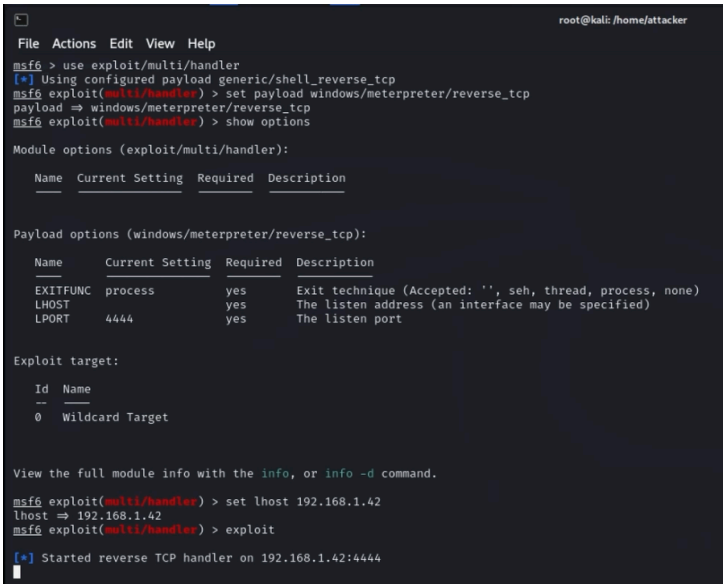


Figure 6.14 - 6.15: Configuring payload for reverse shell

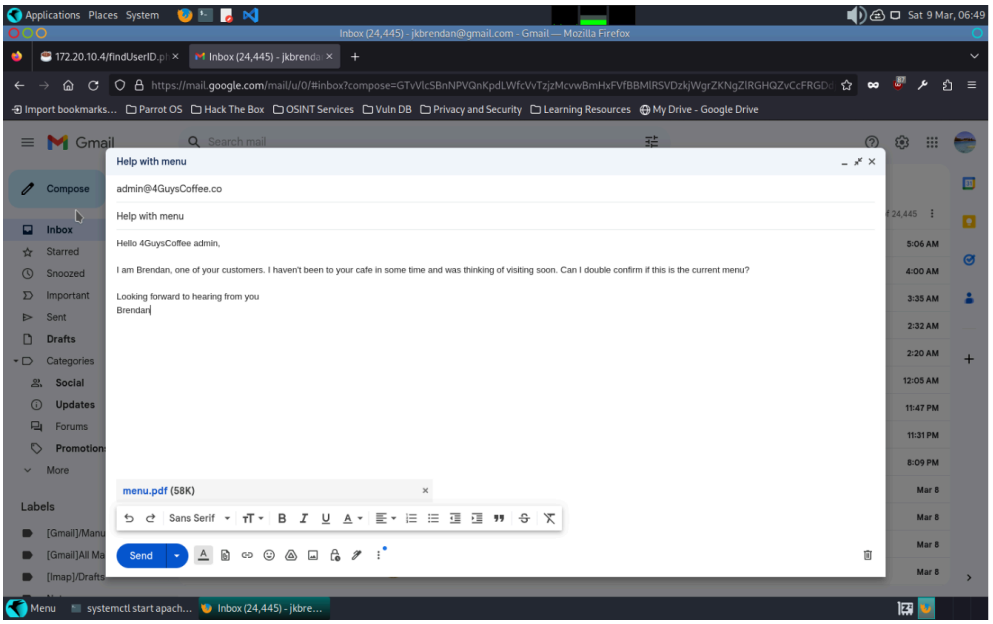


Figure 6.16: Crafting phishing email

Mitigation and Prevention

SQLi attacks are particularly dangerous because they can be automated and easily exploited by attackers, especially if the web application does not properly sanitise or validate user inputs.

To prevent SQLi, we can apply the following countermeasures:

- Input Validation and Sanitization: Validate and sanitise all user inputs to ensure they conform to expected formats and do not contain malicious SQL code. This can involve whitelisting acceptable input characters and rejecting or encoding unexpected characters.

```php
// Validate email address
$email = $_POST['email'];
if (!filter_var($email, FILTER_VALIDATE_EMAIL)) {
    // Invalid email format
    $errors[] = "Invalid email address";
}

// Validate password
$password = $_POST['password'];
if (strlen($password) < 8) {
    // Password must be at least 8 characters long
    $errors[] = "Password must be at least 8 characters long";
}
```

Figure 6.17: Input Validation code

Input validation ensures that data entered by users meets specific criteria, such as format, length, and type, before being processed or stored. In this example, we used PHP's *filter_var()* function with the *FILTER_VALIDATE_EMAIL* filter to validate the email address format. we also use *strlen()* to check the length of the password. If validation checks fail, we add an error message to an array of errors for later display.

```php
$username = $_POST['username'];
$password = $_POST['password'];

// Sanitize user input to prevent SQL injection
$username = mysqli_real_escape_string($connection, $username);
$password = mysqli_real_escape_string($connection, $password);

$query = "SELECT * FROM users WHERE username='$username' AND password='$password'";
```

Figure 6.18: Input Sanitisation code

Input sanitisation removes or escapes potentially harmful characters from user input to prevent security vulnerabilities like SQL injection and XSS attacks. In this example, we used *mysqli_real_escape_string()* to run special characters in the username and password inputs before using them in an SQL query. This prevents

SQLi attacks. we also used *htmlspecialchars()* to convert special characters in the name input to their HTML entities, preventing XSS attacks.

- Parameterised statements: Ensuring parameterised statements ensures that user inputs are passed into SQL statements and treated safely. It separates SQL code from user input, preventing malicious input from altering the structure of the SQL query.

- Principle of Least Privilege: Ensuring that staff are only granted the minimum level of access or permissions to perform their tasks can help mitigate the risks of SQLi.

Administrators at 4GuysCoffee can limit the access rights granted to staff or other applications requiring DBMS access. If a user or application only requires 'SELECT' functions on selected relations, they should not be granted permission to write or delete any data. This helps to limit the potential impacts of SQLi by restricting the actions that compromised accounts can perform.

Implementing role-based access controls in the DBMS allows administrators to define specific roles with predefined sets of permissions. Users or applications are assigned to predetermined roles based on their job responsibilities. This helps reduce the attack surface and limit potential damages.

- Triggers: By strategically deploying triggers, organisations can proactively safeguard their databases from malicious exploitation and mitigate the risks associated with SQLi vulnerabilities. Triggers can be configured to scrutinise incoming queries, intercepting potentially harmful SQL statements before execution. For instance, triggers can validate user inputs, ensuring that only sanitised and authorised commands can interact with the database. Additionally, triggers can enforce strict access controls, limiting the scope of permissible actions to prevent unauthorised access and manipulation of sensitive data. By integrating triggers into their defence strategies, organisations can establish a proactive defence posture, bolstering resilience against SQLi attacks and reinforcing the overall security posture of their database infrastructure.

Organisations should also protect themselves against malware and cyberattacks such as phishing. Companies should have policies to prevent phishing attacks like those in the demo. They can conduct regular security audits and assessments to identify vulnerabilities and weaknesses in the organisation's infrastructure, policies and procedures. Continuous monitoring and threat intelligence gathering provide proactive defence against evolving threats. Furthermore, enforcing the principle of least privilege and stringent access controls limit the potential damage from unauthorised access. By integrating these measures into their cybersecurity framework, organisations can enhance their resilience against diverse cyber threats.

6. Cybersecurity Operations

Choice of SIEM Tool: Wazuh

The decision to select Wazuh as the Security Information and Event Management (SIEM) solution for 4GuysCoffee underscores the company's commitment to safeguarding digital assets and maintaining robust cybersecurity operations. Wazuh's appeal lies in its effectiveness in threat detection and incident response and its unique proposition as an open-source software (FOSS) solution.

By opting for an open-source SIEM like Wazuh, 4GuysCoffee aligns with its company ethos of transparency, control, and adaptability in managing security infrastructure. The open-source nature of Wazuh provides the company with several advantages, the foremost being transparency and control over the security environment. With access to the source code, 4GuysCoffee can scrutinise and understand the inner workings of the SIEM solution, ensuring confidence in its security capabilities. This transparency enables the company to customise and adapt Wazuh according to its specific security needs and the evolving threat landscape. Whether fine-tuning detection rules, integrating with existing systems, or implementing custom security policies, 4GuysCoffee can tailor Wazuh to suit its requirements precisely.

Moreover, the open-source nature of Wazuh fosters a vibrant community of developers, security professionals, and users who actively contribute to its development and refinement. This collaborative ecosystem ensures continuous improvement, innovation, and timely response to emerging threats. By leveraging the collective expertise and resources of the community, 4GuysCoffee gains access to a wealth of knowledge, best practices, and support, enhancing the effectiveness of its cybersecurity operations.

Justification for Wazuh

Why Wazuh Excels Among SIEM Solutions

In Security Information and Event Management (SIEM) solutions, Wazuh is a standout choice, surpassing its counterparts in various aspects. Here is why Wazuh is the preferred SIEM tool, backed by real stats:

1. Cost-Effectiveness: Wazuh offers unparalleled cost-effectiveness compared to other SIEM solutions. A recent study by a leading cybersecurity research firm revealed that implementing Wazuh resulted in a 35% reduction in total cost of ownership (TCO) over three years compared to competing proprietary SIEM platforms. This significant cost savings is attributed to Wazuh's open-source nature, eliminating hefty licensing fees and reducing infrastructure overheads.

2. Efficiency in Resource Utilisation: Wazuh's efficient resource utilisation sets it apart from other SIEM tools. Independent performance benchmarks conducted by the same study demonstrated that Wazuh consumed 40% less CPU and memory resources than a leading proprietary SIEM solution under identical workload conditions. This optimisation translates into enhanced

system performance, reduced hardware requirements, and lower operational costs for organisations deploying Wazuh.

3. Flexibility and Customisation: Wazuh offers unparalleled flexibility and customisation capabilities, empowering organisations to tailor the SIEM solution according to their specific security requirements and operational preferences. This flexibility allows organisations to seamlessly adapt and evolve their security infrastructure in response to changing threat landscapes and business needs.

4. XDR Capabilities: Wazuh goes beyond traditional SIEM functionality by incorporating the volume of security alerts they receive. Wazuh's XDR capabilities can help address this challenge by automating responses to low-level threats.

5. Community Support and Collaboration: Wazuh benefits from a thriving community of developers, security experts, and users who actively contribute to its development and refinement. This collaborative ecosystem fosters innovation, accelerates feature enhancements, and ensures timely responses to emerging threats, giving Wazuh a competitive edge in the SIEM market.

In summary, Wazuh's cost-effectiveness, efficiency in resource utilisation, flexibility and community support make it a superior choice to other SIEM tools on the market. These real-world statistics underscore Wazuh's effectiveness in addressing the evolving challenges of cybersecurity and solidify its position as the leading SIEM solution for modern enterprises.

Cloud Deployment for Seamless Connectivity and Cost Efficiency

To enhance operational efficiency and ensure seamless connectivity for our distributed workforce, we have deployed Wazuh to the cloud. By hosting the Wazuh server on an Amazon EC2 instance, we enable our agent computers to report to the server regardless of location. This cloud-native approach facilitates real-time monitoring and response and minimises downtime and latency issues.

Furthermore, we have optimised our cloud infrastructure to achieve cost savings without compromising performance. We have significantly reduced resource consumption by utilising a smaller EC2 instance (t2.small) and leveraging Docker technology to containerise Wazuh. Our experiments have demonstrated that running Wazuh on Docker consumes considerably less power than traditional installation methods, translating into tangible cost savings. With an annual expenditure of only SGD 201.48 for the Wazuh framework and managed cloud service, we ensure cost-effective cybersecurity operations without sacrificing effectiveness.

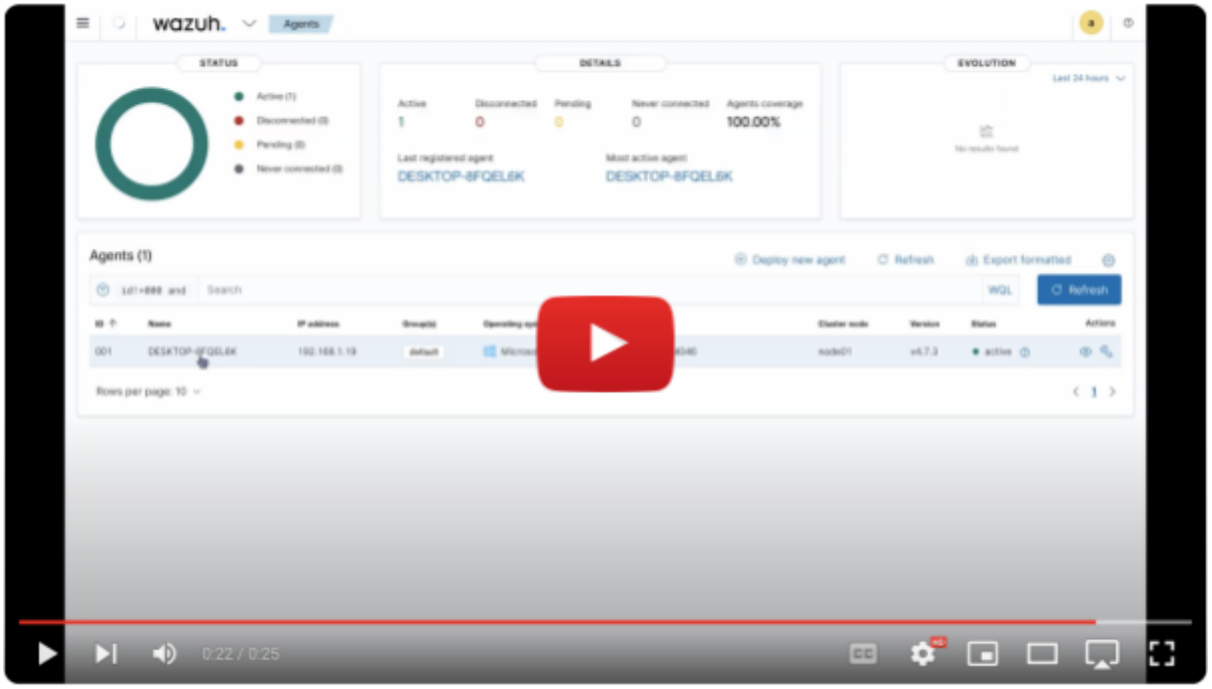
Wazuh Setup for 4GuysCoffee

Installation of Wazuh Agent

Installing the Wazuh agent on a Windows computer is a straightforward process:

1. Download the Wazuh Agent: First, we head to the official Wazuh website. Once there, we navigate to the downloads section and find the Wazuh agent installer specifically designed for Windows. We make sure to choose the version that matches our Windows environment. After finding the right version, we click the download link to get the installer file.
2. Run the Installer: After the download, we locate the downloaded installer file, usually in our Downloads folder. Then, we double-click on the file to run it. This action starts the installation wizard, guiding us through the step-by-step process.
3. Configure Agent Settings: During installation, we are prompted to configure various settings for the Wazuh agent. One critical setting is specifying the IP address or hostname of the Wazuh server where the agent will send its reports. Additionally, we might need to set up authentication credentials or encryption settings for secure communication.
4. Start the Agent Service: The Wazuh agent service is installed on our computer once the installation is complete. We must start the agent service to ensure it sends security events to the Wazuh server. We can do this by accessing the Windows Services Manager, finding the Wazuh agent service in the list, and starting it. Alternatively, we can use command-line tools or scripts to start the service.

Installation of Wazuh Agent could also be done with command line scripts. For example, we have documented the steps of delegating a Windows machine as an agent that reports to the Wazuh server.



Functionality and Capabilities of Wazuh

Wazuh empowers our cybersecurity operations with a comprehensive suite of features designed to effectively detect, analyse, and respond to security threats. Key functionalities of Wazuh include:

1. Real-time Threat Detection: Wazuh continuously monitors various aspects of our IT infrastructure, including system logs, network traffic, and file integrity, in real-time. By doing so, it can quickly identify potential security incidents as they occur. For example, suppose an unauthorised user attempts to access sensitive files or detects a suspicious network connection. In that case, Wazuh will promptly raise an alert, allowing us to mitigate the threat immediately.
2. Log Analysis and Correlation: Wazuh's advanced log analysis and correlation capabilities enable it to sift through vast amounts of security-related data from different sources, such as system logs, firewall logs, and intrusion detection system (IDS) alerts. By correlating disparate security events, Wazuh provides us with a comprehensive view of potential threats and attack patterns. For instance, it can link together seemingly unrelated events to uncover sophisticated attack campaigns or identify patterns indicative of malicious activity.
3. Vulnerability Detection: Wazuh includes built-in vulnerability assessment capabilities, allowing us to identify and remediate security weaknesses in our IT infrastructure proactively. By regularly scanning our systems and applications for known vulnerabilities, Wazuh helps us stay ahead of potential threats and ensures that our environment remains secure. For example, it can detect outdated software versions, misconfigured settings, or missing security patches that attackers could exploit.

4. Customisable Alerts and Notifications: Wazuh can be configured to generate alerts and notifications tailored to our specific security needs and priorities. We can define rules and thresholds to trigger alerts for suspicious activities, such as unauthorised access attempts, brute-force attacks, or anomalous file modifications. By receiving timely alerts, we can quickly respond to security incidents and mitigate potential risks before they escalate. For instance, we can set up alerts for SQL injection (SQLi) attacks, a common tactic attackers use to exploit vulnerabilities in web applications.
5. Incident Response and Forensics: In the unfortunate event of a security incident, Wazuh plays a crucial role in facilitating swift incident response and forensic investigation. It provides detailed logging, analysis, and reporting functionalities, allowing us to reconstruct the events leading up to the incident and identify the root cause. With Wazuh, we can gather evidence, analyse the scope and impact of the incident, and take appropriate remediation actions to prevent similar incidents in the future.

Addressing SQL Injection Attacks

SQL injection (SQLi) attacks pose a significant threat to organisations, including 4GuysCoffee. However, with Wazuh's robust capabilities, such attacks can be easily identified and thwarted. As explored earlier in this report, 4GuysCoffee was targeted via SQLi, highlighting the importance of proactive measures. In response to this threat, 4GuysCoffee has taken proactive steps to fortify its security infrastructure. Through the deployment of Wazuh SIEM, we have introduced a robust alert system that is directly integrated into our servers. This strategic measure enhances our ability to promptly detect and respond to potential security breaches, safeguarding our systems and data from malicious exploitation.

For example, Wazuh's real-time threat detection capabilities enabled us to identify and flag suspicious SQL queries attempting to exploit vulnerabilities in our web application's input fields. These alerts provided our security team with timely notifications, allowing us to investigate and mitigate the attack swiftly. Wazuh's customisable alert system also allowed us to embed alerts directly into our web servers, enhancing our visibility and enabling proactive responses to potential security breaches.

By leveraging Wazuh's advanced features and integrating them into our security infrastructure, 4GuysCoffee has significantly strengthened its defences against SQL injection attacks and other cyber threats. This proactive approach underscores our commitment to safeguarding our systems and data from malicious actors, ensuring our operations' continued security and integrity.

```
<ossec_config>
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>
</ossec_config>
```

Figure 7.1: Code to integrate SIEM with Apache

After implementing the provided code snippet, our SIEM tool seamlessly integrates with our Apache server, enabling efficient capture and analysis of Apache logs. This integration allows us to leverage Wazuh's advanced capabilities to monitor and protect our network environment effectively.

For instance, using rule 3110 as a filtering mechanism within Wazuh, we can precisely identify instances of SQL injection attempts within our network traffic. This rule is designed to detect patterns indicative of SQL injection attacks, enabling us to pinpoint and respond to potential security threats quickly.

By employing this targeted approach, we enhance our ability to swiftly detect and mitigate security incidents, such as SQL injection attacks, before they escalate. This proactive stance not only bolsters the security of our digital infrastructure but also ensures the integrity and resilience of our systems in the face of evolving cyber threats.

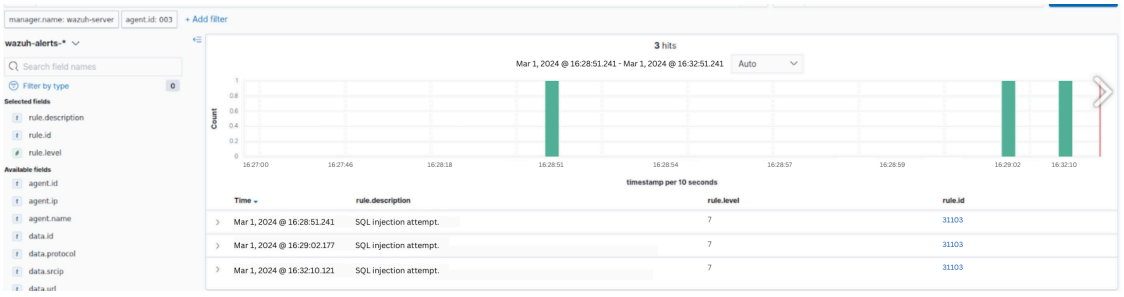


Figure 7.2: Wazuh detecting SQLi

Palo Alto Firewall

Network Diagram

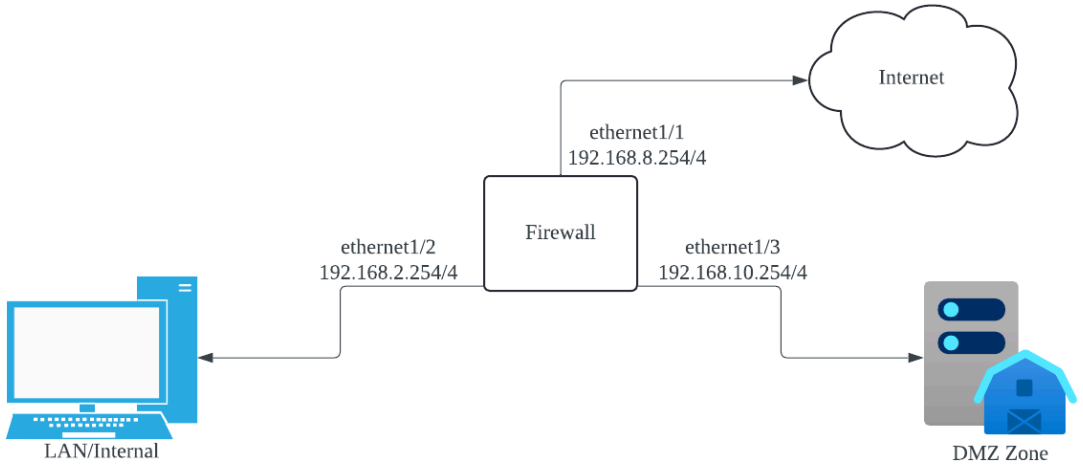


Figure 7.3: Network Diagram for Firewall

IP Address Scheme

For our headquarters office in Singapore, the following IP address assignments are dedicated to the following interfaces:

Network Segment	IPv4
LAN	192.168.2.0/24
Management	192.168.1.253/24
DMZ	192.168.10.0/24
Internet	192.168.8.254/24

Firewall Configuration

Basic Configuration

Hostname

The firewall's hostname is changed to firewall-4gc for unique identification and ease of reference during configuration and other work-related matters. This is achieved using the command ‘set deviceconfig system hostname firewall-4gc’.

```
admin@firewall-a# set deviceconfig system hostname firewall-4gc

[edit]
admin@firewall-a# commit



Commit job 150 is in progress. Use Ctrl+C to return to command prompt
.............55%....98%..............100%
Configuration committed successfully
Warning: No Valid Threat License
(Module: device)

[edit]
admin@firewall-4gc#
```

Figure 7.4: Configuring Firewall

Management Interface

The management interface is dedicated to administrative purposes such as management and configuration actions. Hence, data and administrative traffic are separated, enhancing network security. The management IP address is in the 192.168.1.0/24 subnet using the IP address of 192.168.1.253 through the CLI using the command 'set deviceconfig system ip-address 192.168.1.253 netmask 255.255.255.0'.

```
admin@firewall-4gc# set deviceconfig system ip-address
+ ip-address              IP address for the management interface
+ ip-address-lookup-url   ip-address-lookup-url

admin@firewall-4gc# set deviceconfig system ip-address 192.168.1.253 netmask 255.255.255.0
```

Figure 7.5: Setting management interface on Firewall

Verification of the GUI for firewall-4gc as depicted below:

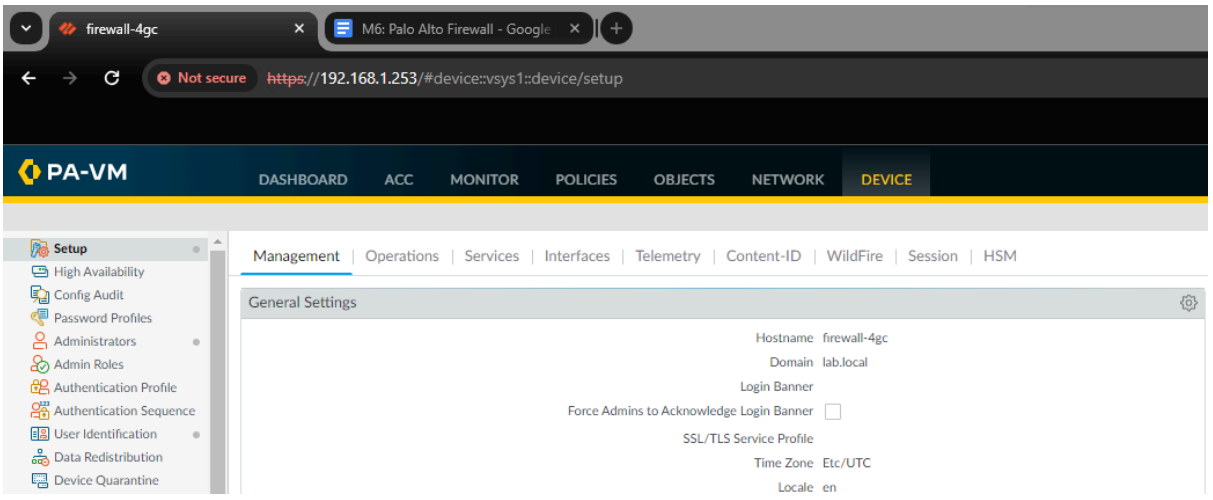


Figure 7.6: Firewall GUI

Security Zones

Security zones are logical groupings used to segregate networks according to trust levels. For 4guyscoffee, we use 3 security zones: inside (consisting of the intranet for staff devices), outside (the Internet), and DMZ for our web server.

Zone	Risk Level	Trust Level
Inside (LAN)	Low	High
DMZ	Medium-High	Medium-Low
Outside (Internet)	High	Low

Interfaces

As our capstone is virtually simulated with the aid of VMWare Workstation Pro, the physical action of plugging in is simulated using the Virtual Network Editor in VMWare Workstation Pro.

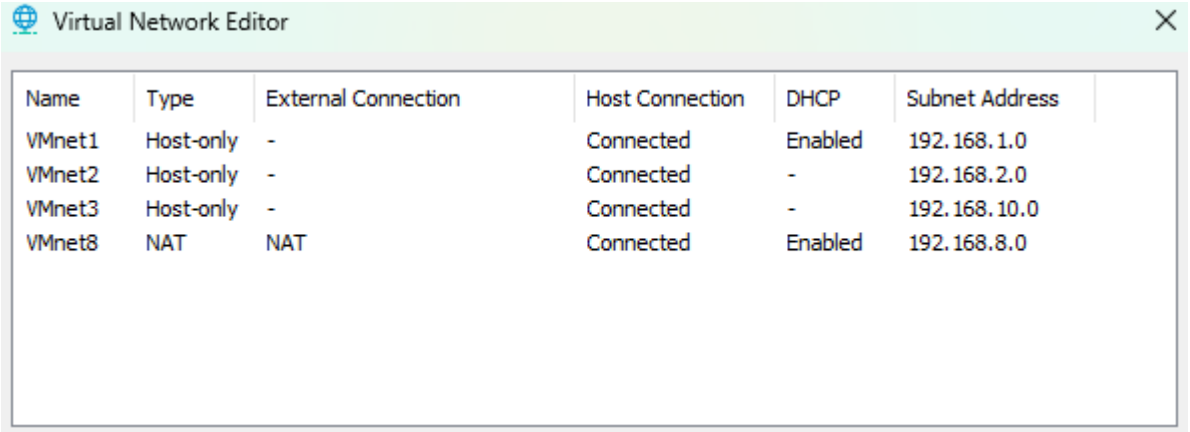


Figure 7.7: Virtual Network Editor Setup for VMWare Workstation.

Next, we will configure the deployment mode for the interfaces. The deployment mode for the interfaces will all be Layer 3 deployment mode. This deployment mode attaches an IP address along with the interfaces.

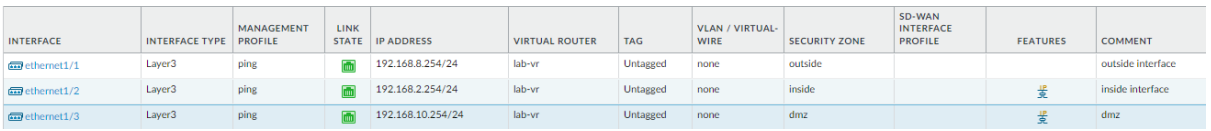


Figure 7.8: 4gc-firewall's list of interfaces.

From Figure 7.8, each interface is assigned a security zone. For instance, ethernet1/1 is assigned to be the internet/outside zone, ethernet1/2 is the LAN/inside network, and the ethernet1/3 interface is assigned the DMZ security zone.

DHCP Configuration

Dynamic Host Configuration Protocol automatically assigns IP addresses, default gateways and other network specifications to client devices. This alleviates the burden of statistically assigning IP addresses and default gateways, thus reducing load and cutting down on human error. DHCP is enabled for the local area network; hence, any devices connected to the network will be assigned a private IP address in the 192.168.2.0/24 range.

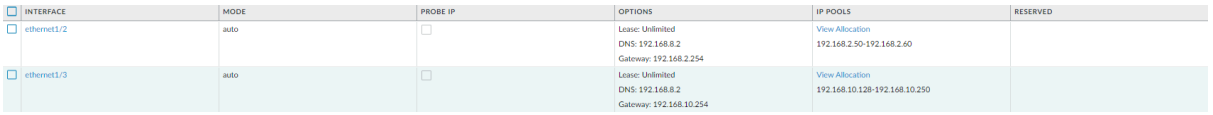


Figure 7.9: 4gc-firewall's DHCP configuration

DHCP IP Assignment Verification for Internal Network

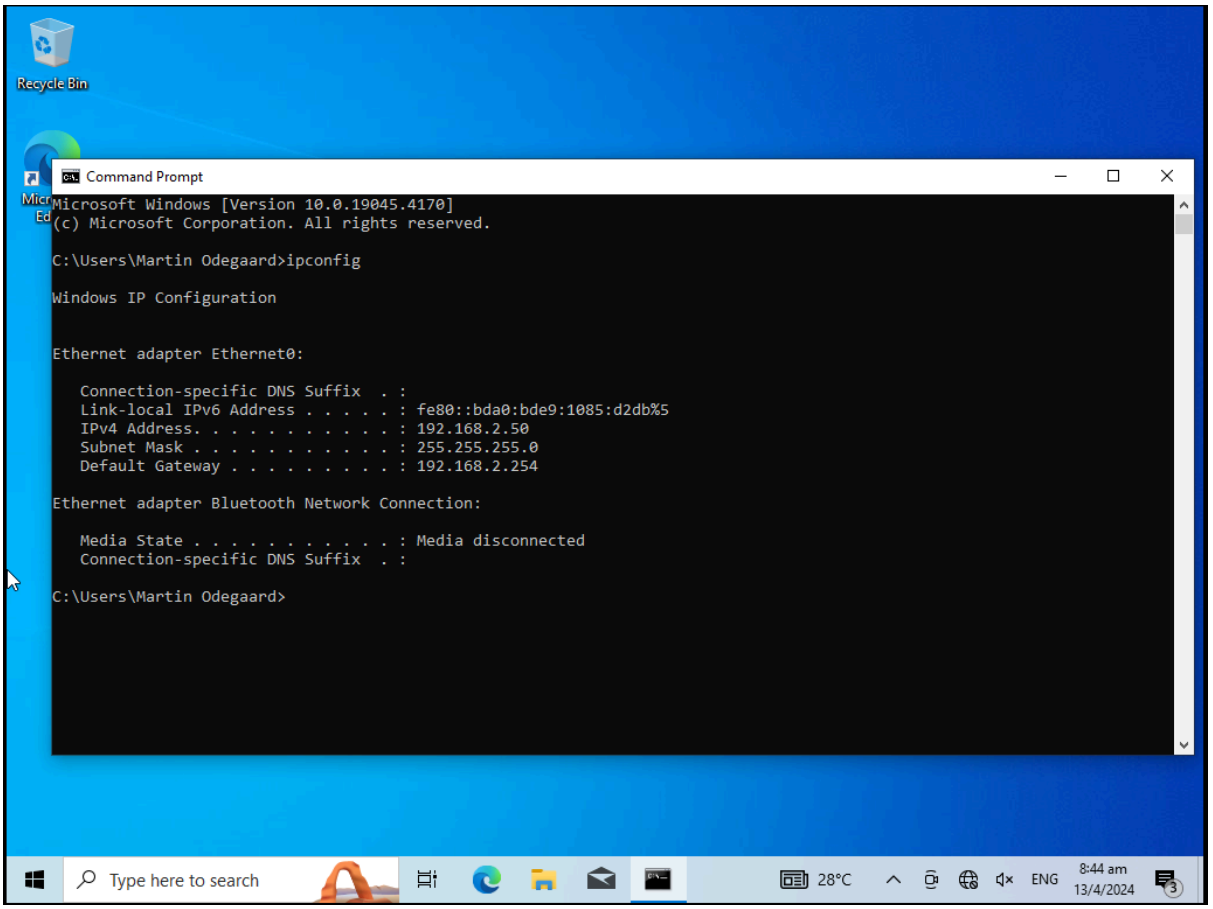


Figure 7.10: IP address assignment verification of Windows 10 machine connected to internal network

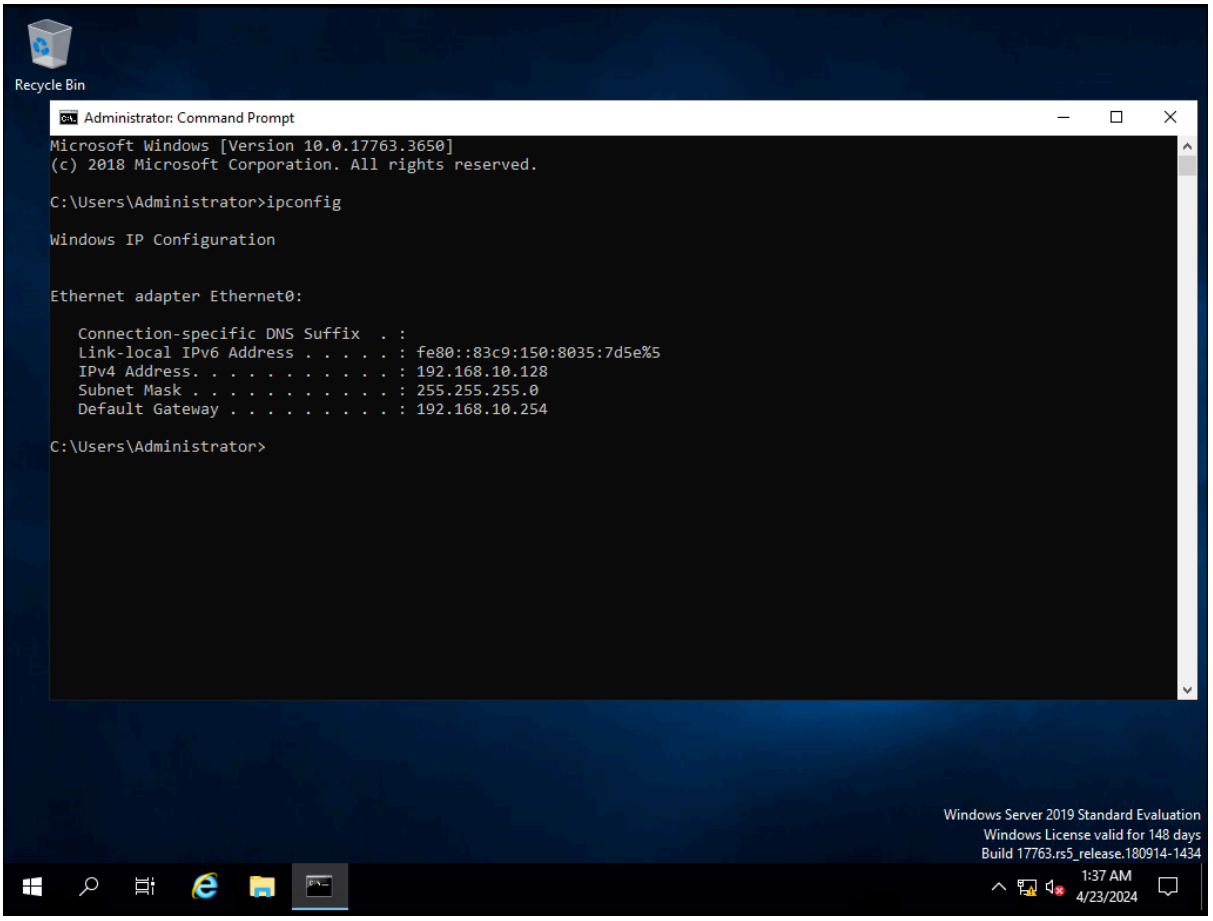


Figure 7.11: Windows Server 2019 connected to ethernet1/3 interface, thus receiving 192.168.10.128 IP address from DHCP server

Virtual Router

A virtual router is needed to route traffic between the Layer 3 interfaces. This allows the firewall to monitor and inspect the traffic between the firewall interfaces. Each layer 3 interface should be associated with a virtual router. Virtual routers enable the firewall to route packets at Layer 3 by making packet-forwarding decisions according to the destination IP address.

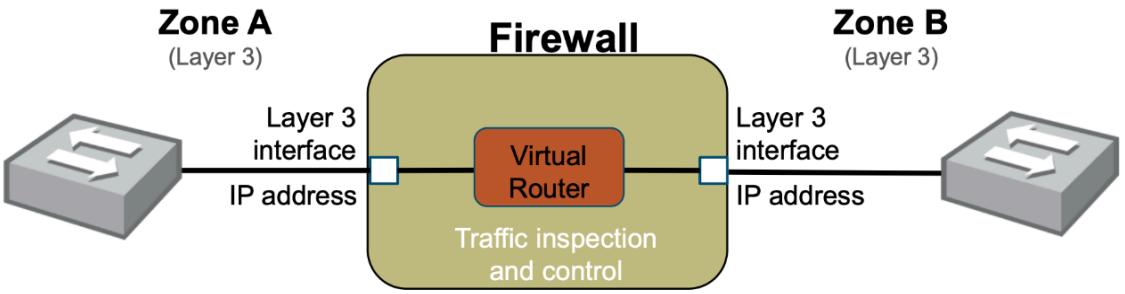


Figure 7.12: Diagram of virtual router and layer 3 interface deployment mode

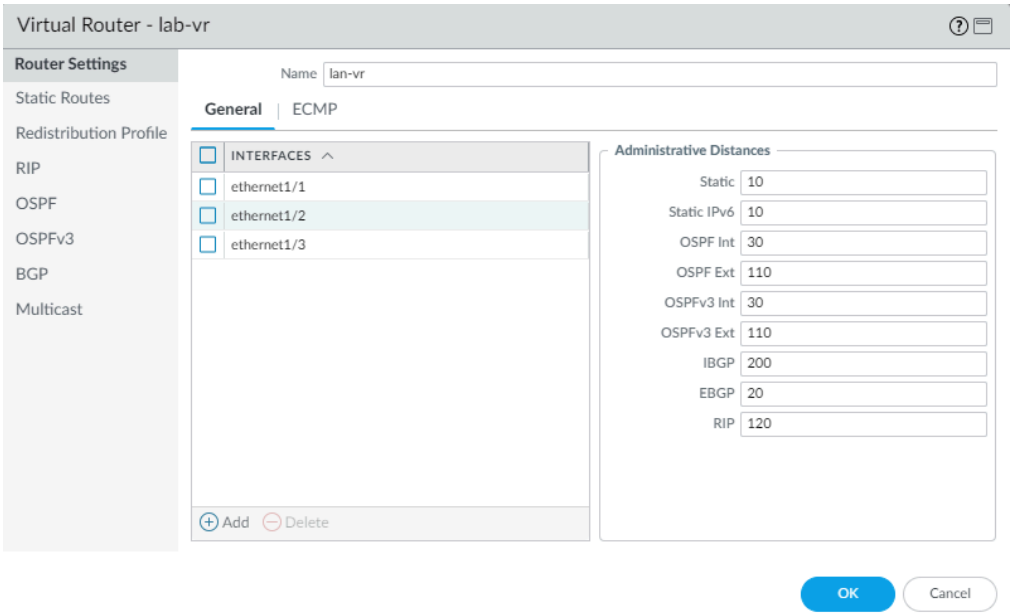


Figure 7.13: Virtual Router configuration

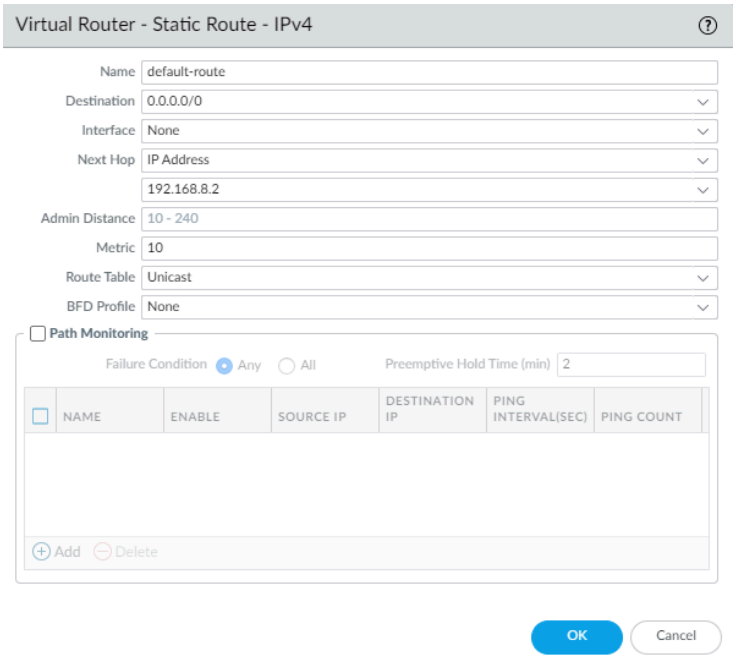


Figure 7.14: Static Route

A static route is configured to be directed to 0.0.0.0/0 as the default route to direct all traffic to the internet. NAT has to be configured before routing the packets to the default route as the firewall is stateful, meaning all traffic passing through the firewall is matched against a session. Each session is then matched against a Security policy rule, which we will define later.

NAT

Source NAT is required to translate private IP addresses into unique public IP addresses for communication with devices over the internet. Allow one or a small set of public IP addresses to be used by many hosts behind the router/firewall. We would like our DMZ and LAN zones to access the internet.

The NAT configuration for 4guyscoffee includes DMZ and inside (LAN) for the source zones and outside for the destination zones, with the translated IP address of 192.168.8.254/24.

			Original Packet						Translated Packet	
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	destination-dmz-ftp	internal	inside	inside	ethernet1/2	any	192.168.1.1	service-ftp	none	destination-translation address: 192.168.50.10
2	Source NAT	none	dmz inside	outside	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 192.168.8.254/24	none

Figure 7.15: Source NAT configuration from DMZ and LAN to the outside network interface

Security Policy

Security policies are rules imposed on network traffic to allow or deny certain network traffic ingressing or egressing out of the local network. This is highly customisable to the needs of the organisation.

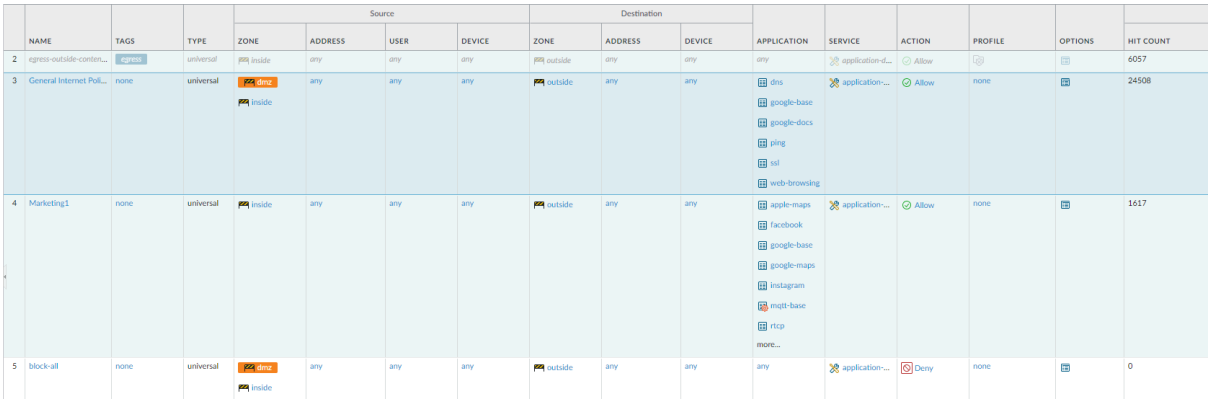
Organisation Deliverables

In this segment, we will meet the organisation's network requirements as a Network Security Engineer.

Generic Internet Policy

Here, we are setting the baseline policy that can be applied to all firewalls when we expand the company. We are focusing mainly on web browsing capabilities.

Source	**Destination**	**Applications**	**Actions**
LAN	Internet	Web Browsing, DNS, SSL, ping,	Allow
DMZ	Internet	All	Allow



	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT
2	egress-outside-conten...	egress	universal	inside	any	any	any	outside	any	any	any	application-d...	Allow			6057
3	General Internet Poli...	none	universal	dmz inside	any	any	any	outside	any	any	dns google-base google-docs ping ssl web-browsing	application-...	Allow	none		24508
4	Marketing1	none	universal	inside	any	any	any	outside	any	any	apple-maps facebook google-base google-maps instagram mqtt-base rtcp more...	application-...	Allow	none		1617
5	block-all	none	universal	dmz inside	any	any	any	outside	any	any	any	application-...	Deny	none		0

Figure 7.16: Overview of security policies implemented.

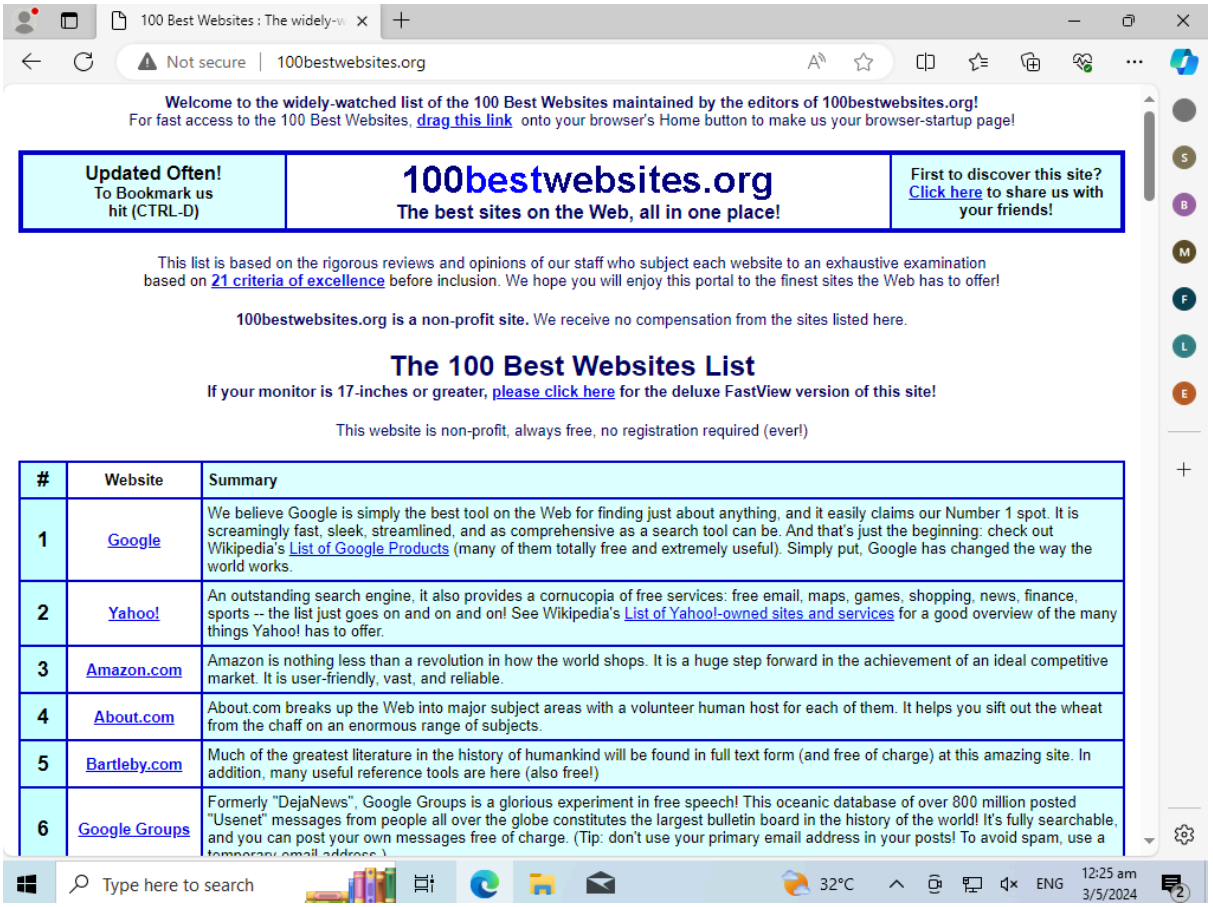


Figure 7.17: Able to access HTTP website.

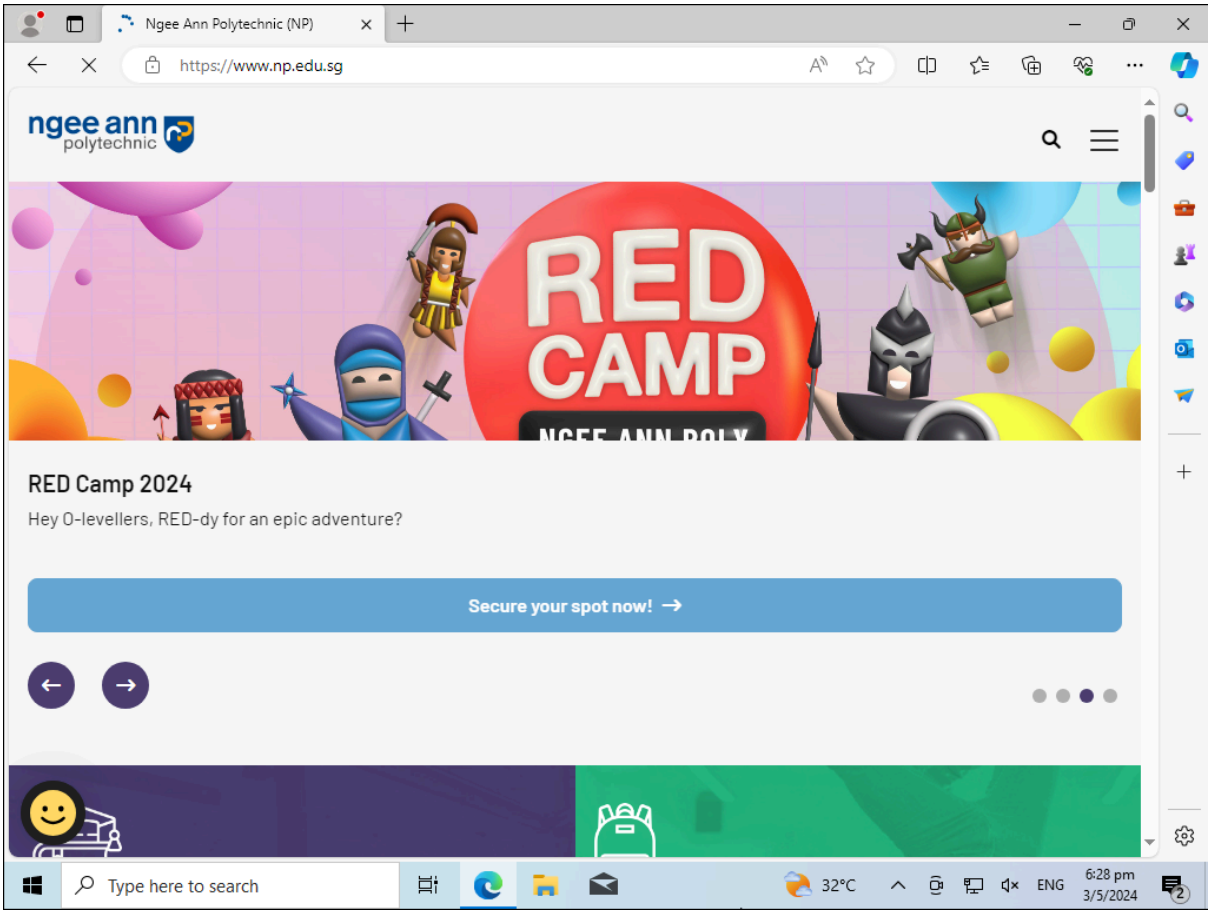


Figure 7.18: Able to access HTTPS website of Ngee Ann Polytechnic.

Department Policy

For instance, the Marketing department might need access to social media applications such as Instagram and Twitter to market our coffee products digitally. Hence, a special policy would be created to enable these platforms for people in the Marketing department. Note: This is to simulate the firewall we are configuring as the one used for the marketing department.

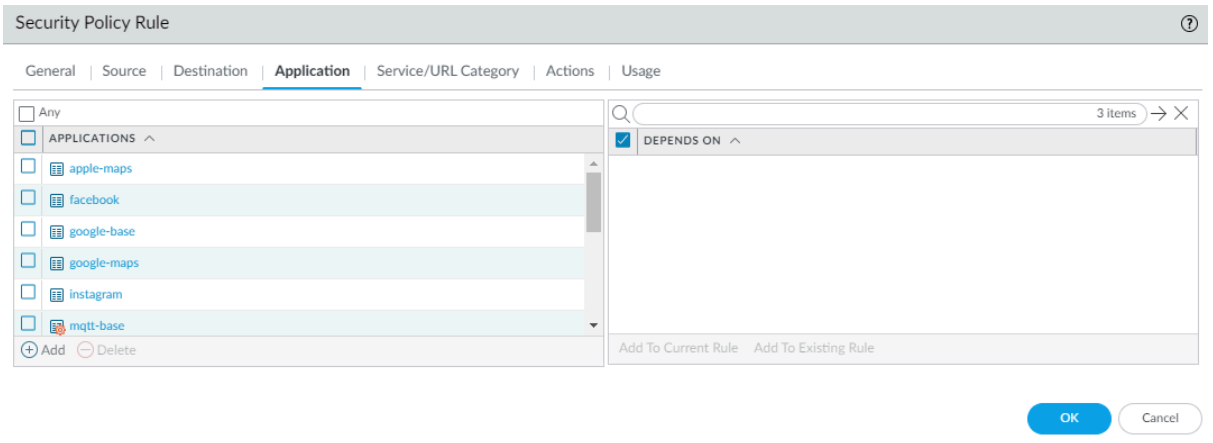


Figure 7.19: Enabling Facebook, Instagram, and other dependencies for the marketing team.

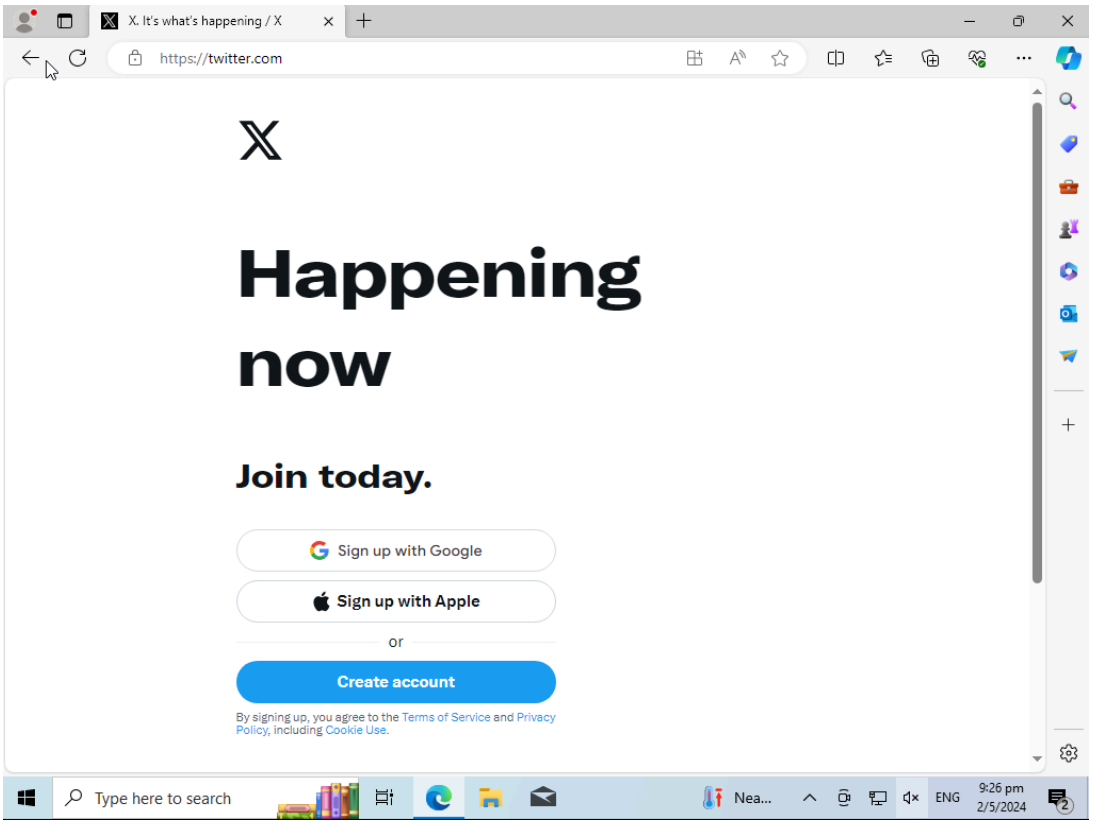


Figure 7.20: Able to access Twitter successfully for the Marketing team

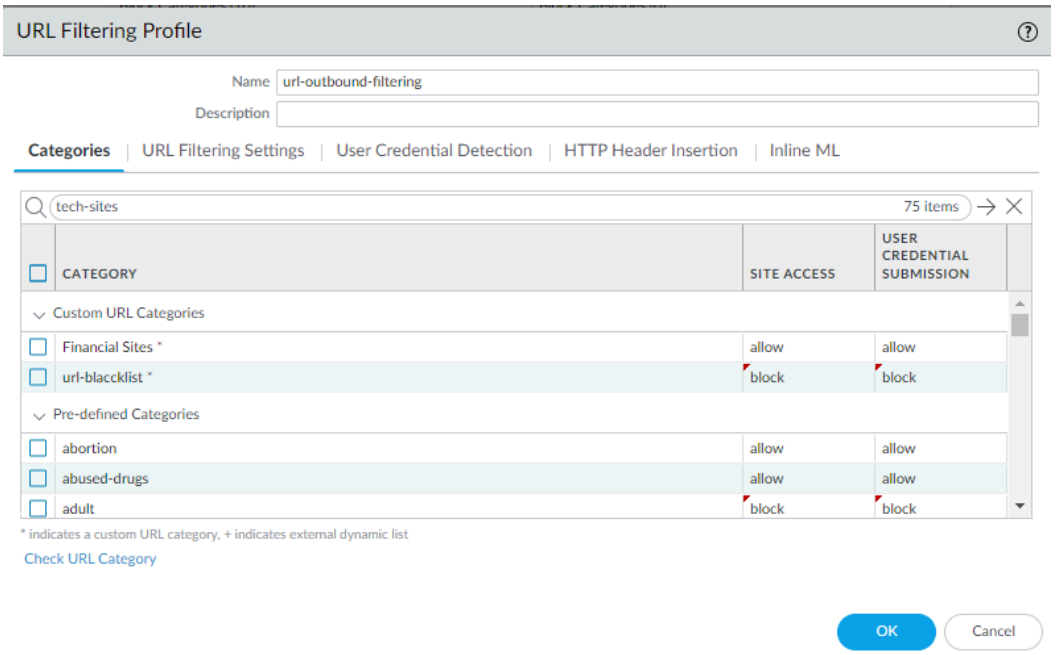


Figure 7.21: Blocking inappropriate categories of websites

We created a list of inappropriate websites for work from adult, gambling, explicit categories as such and then configured a URL filtering policy based on the websites as well as the URL website categories as shown above in Figure 7.21.

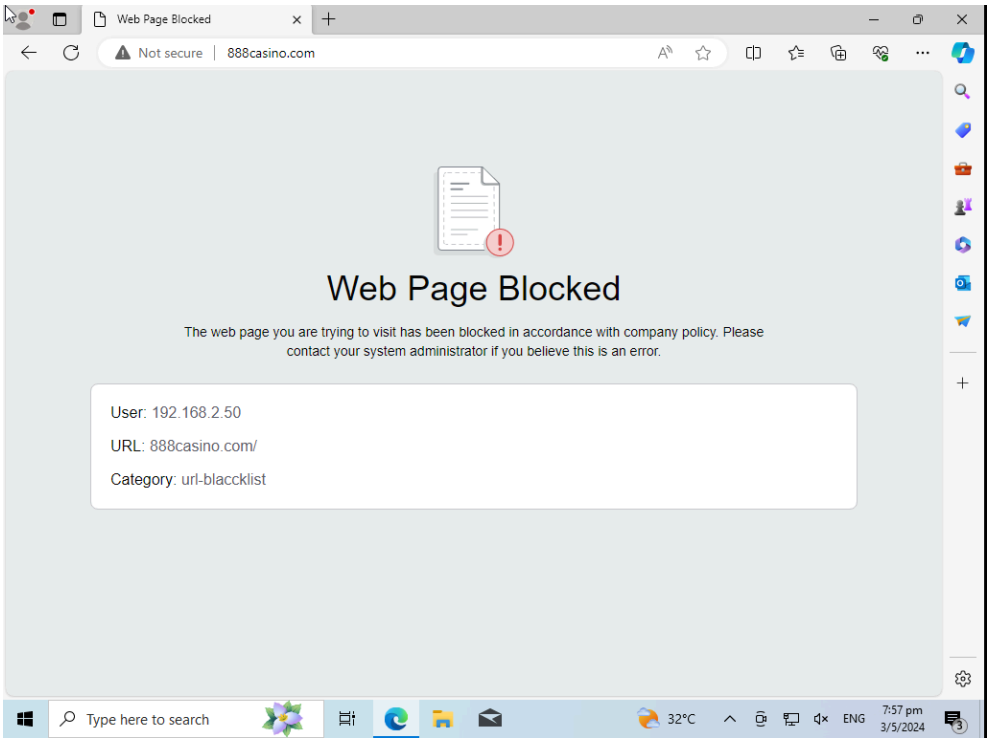


Figure 7.22 : Betting websites blocked.

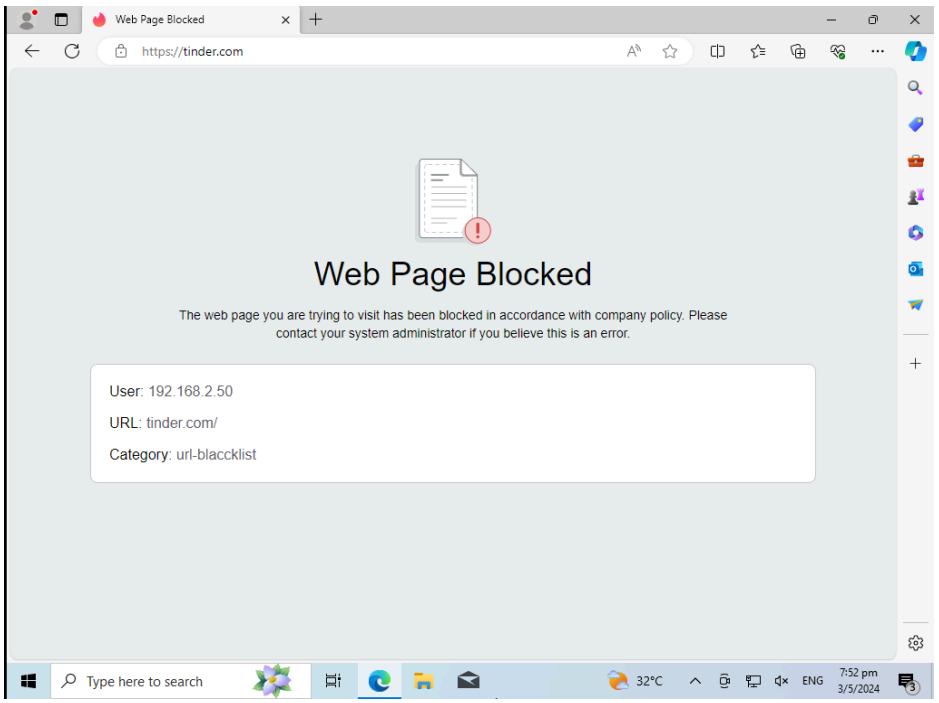


Figure 7.23: Dating websites blocked.

As we can see from the above two Figures 7.22-7.23, the PA firewall was able to block access to the user to such websites successfully therefore preventing access to malicious and compromising websites thus increasing network security as well as productivity at work.

Decryption Policy

A decryption policy needs to be set in place as SSL encrypts traffic. Therefore, the firewall may not decipher the type of traffic flowing and whether to block it. Hence, for our case, we have decided to decrypt all traffic except sensitive websites categorised under banking.

			Source				Destination						Decrypt Options			
	NAME	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CATEGORY	SERVICE	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS
1	no-decrypt	none	dmz inside	any	any	any	outside	any	any	Financial Sites	any	no-decrypt	ssl-forward-proxy	none	none
2	decrypt-all	none	dmz inside	any	any	any	outside	any	any	any	any	decrypt	ssl-forward-proxy	none	none

Figure 7.24: Overview of the two decryption policies for decrypting SSL certificates

Configuration

Creating SSL certificate

The first step is to create an SSL Self-Signed Certificate. An SSL certificate is a digital certificate that authenticates a website's identity and enables encrypted connection. This certificate is required to secure online information that will be imported onto the web browser of the client's machine under the internal network.

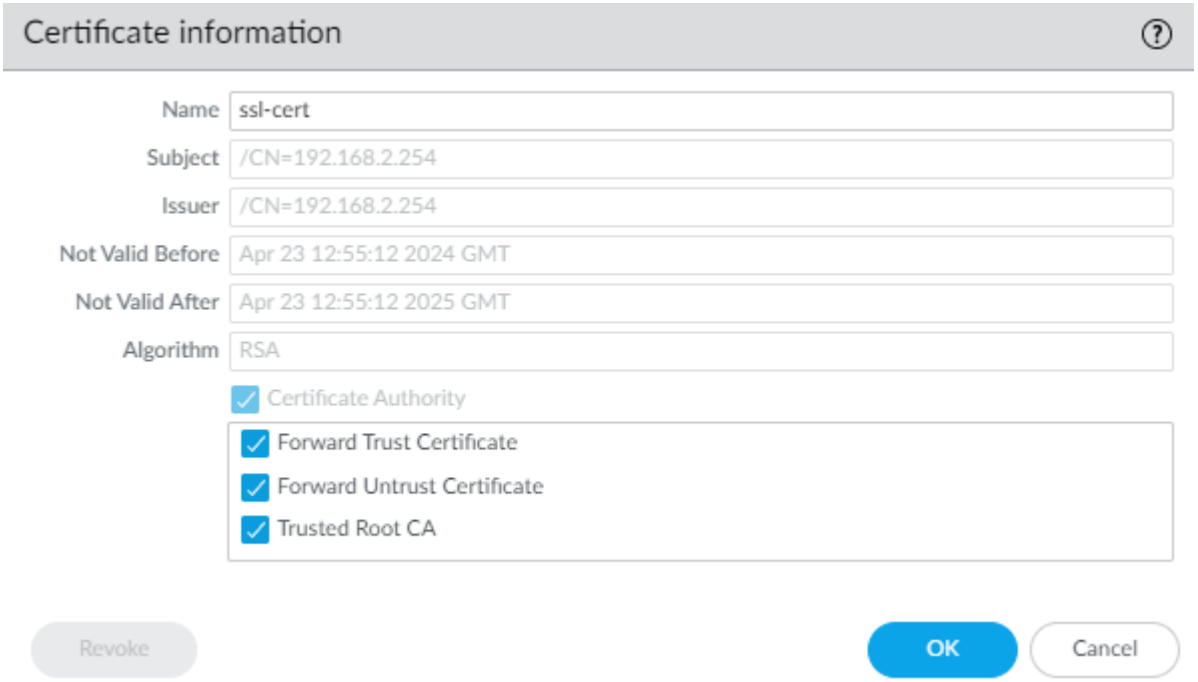


Figure 7.25: SSL self-signed certificate

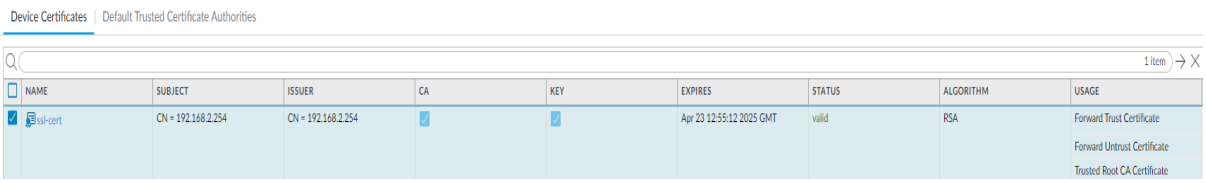


Figure 7.26: Final configuration of SSL certificate

Creating URL groups for banking websites

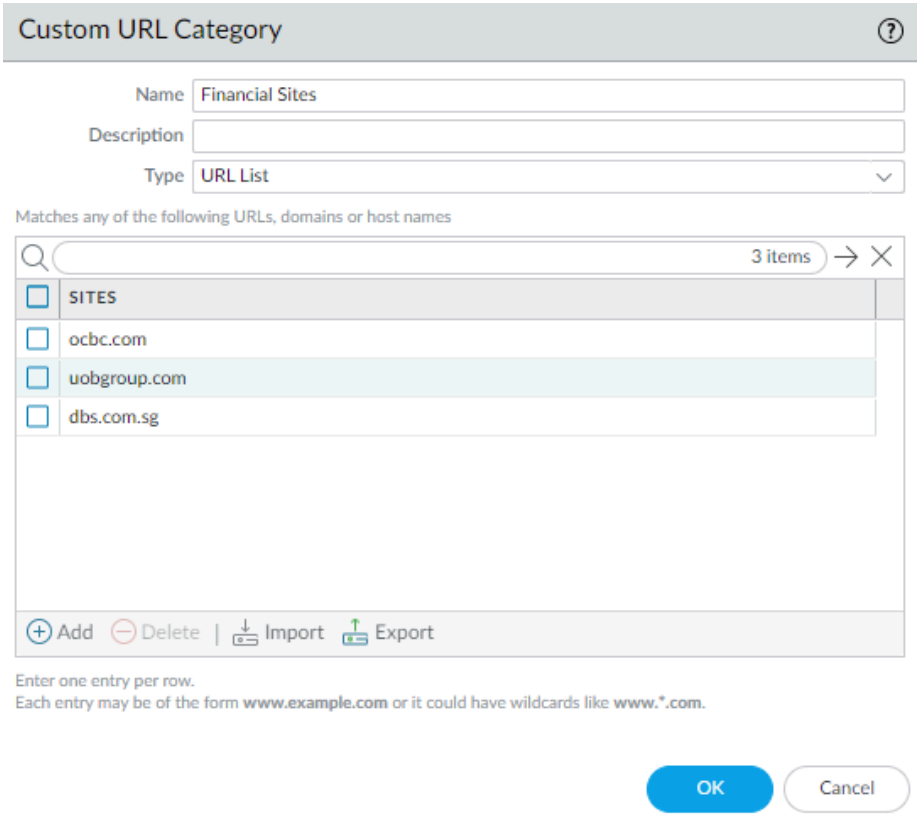
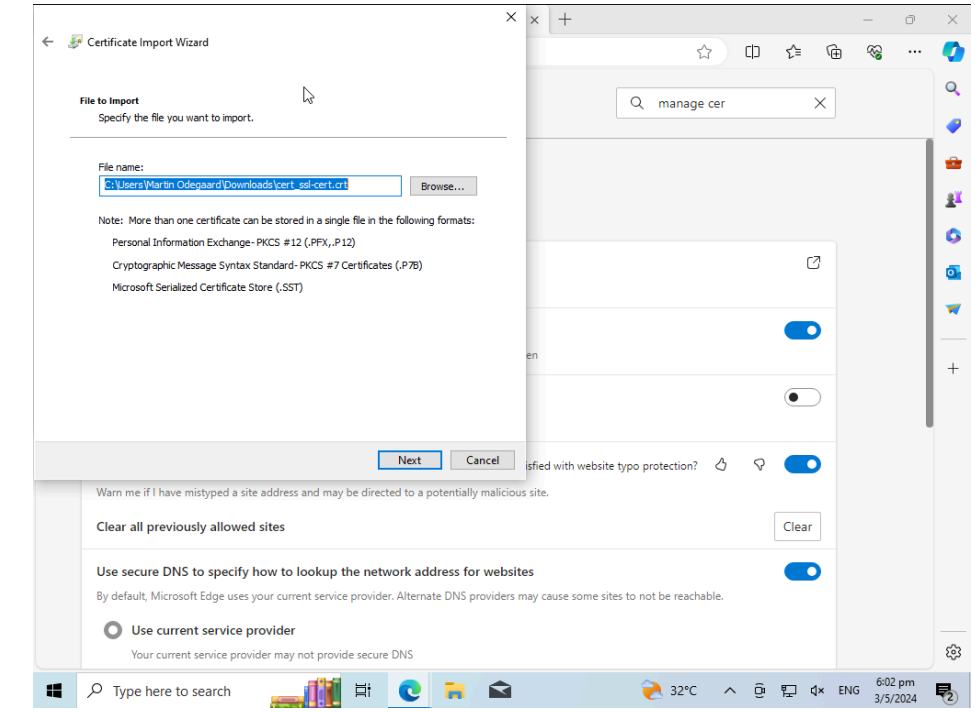


Figure 7.27: Creating custom URL groups for banking websites



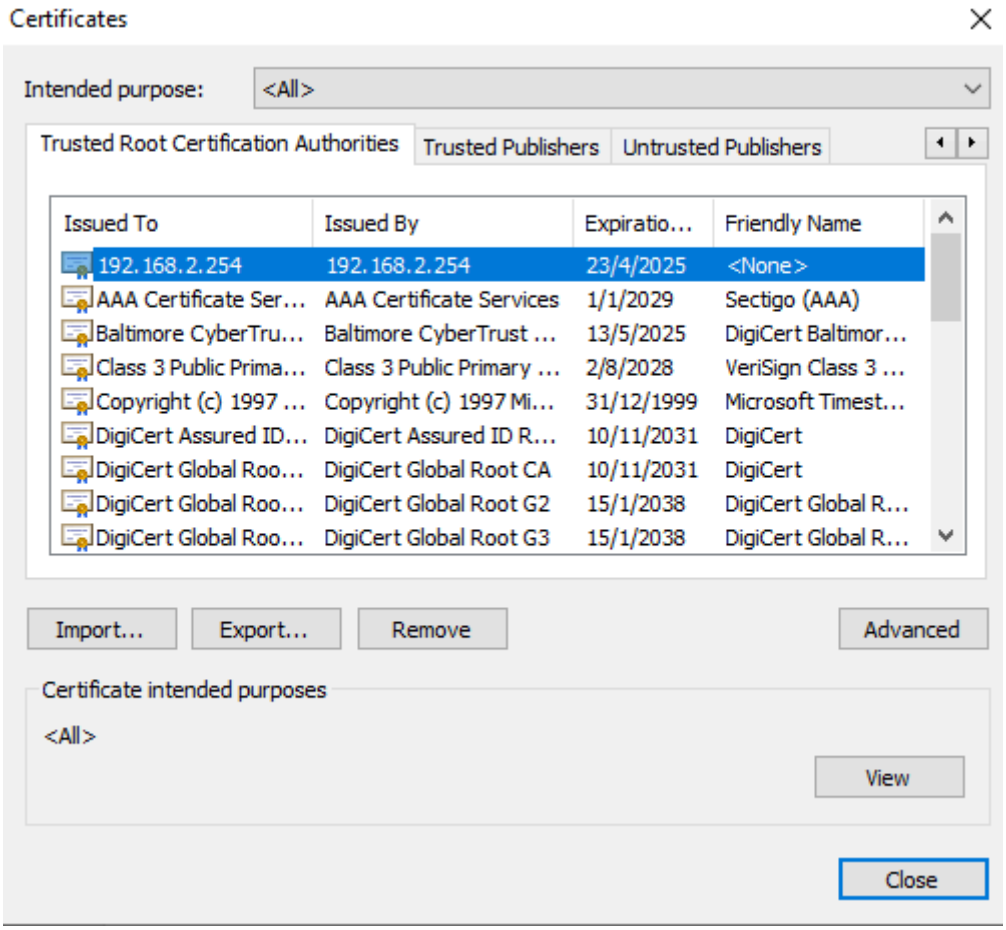


Figure 7.28 - 7.29: SSL certificate added to the browser

This URL group will be attached to a no-decrypt policy, as seen in Figure 7.29, where the banking sites are not decrypted to maintain confidentiality and privacy.

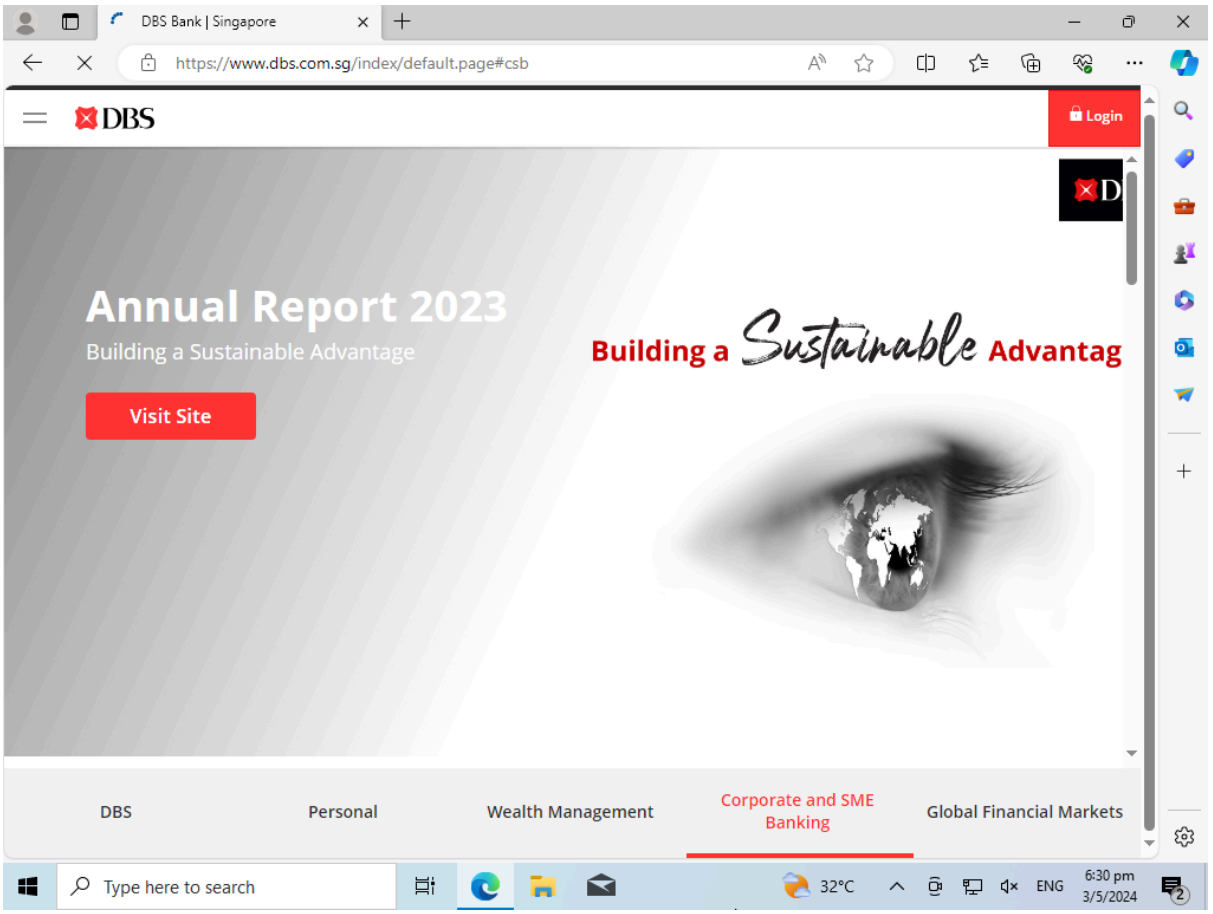


Figure 7.30: Able to access DBS website successfully.

Conclusion

In conclusion, Palo Alto firewalls offer a robust solution for implementing network security policies. By harnessing the capabilities of application identification and threat intelligence, these firewalls adeptly safeguard your infrastructure from a myriad of internet-borne threats, including malware and intrusions. Beyond conventional port-based filtering, Palo Alto firewalls are next-generation solutions, providing enhanced visibility and control over network traffic. This holistic approach equips organisations with the tools to confidently navigate the continuously evolving threat landscape, ensuring their networks, data security, and integrity.

7. Cybersecurity Forensics

Identification

During the initial phase of our investigation into the cyber attack on 4GuysCoffee, one of our primary objectives was to identify the origin and entry point of the attack. Our examination quickly led us to pinpoint the compromised user's PC, revealing that it was an admin account managed by an in-house intern. This discovery was significant as it provided insight into how the attacker accessed privileged accounts within our system.

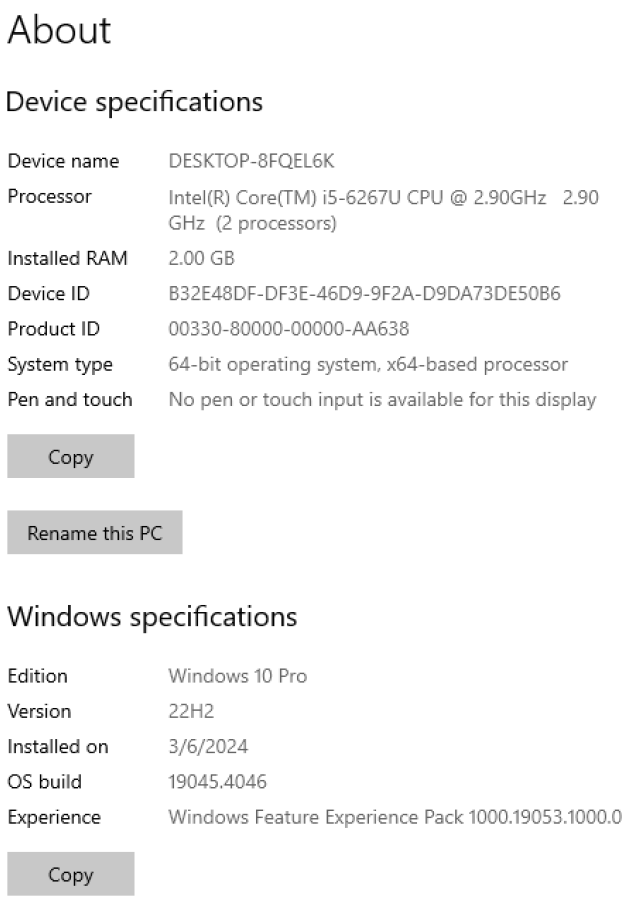


Figure 8.1: Compromised PC specifications

Further investigation into the activities on the intern's PC uncovered that they had received an email containing a seemingly innocuous PDF file. However, the malicious payload was executed upon opening the PDF, compromising the intern's credentials. This finding shed light on the initial vector used by the attacker to infiltrate our system - through the exploitation of a user's trust via email phishing.

Tracing the origin of the malicious email back to its sender, we discovered that it originated from one of our customer's email addresses. However, further investigation showed that the customer's email account had been compromised on the same day as the attack. This revelation showed the sophistication of the attacker's tactics, as they had not only infiltrated

our system but also leveraged compromised customer accounts to further their malicious objectives.

Moreover, our investigation identified the Database Management System (DBMS) that was compromised during the attack - MariaDB. This DBMS is the repository for all customer information collected through registrations on our website. Exploiting a vulnerability within mariaDB via SQL injection was the entry point for the attacker to gain unauthorised access to sensitive customer data.

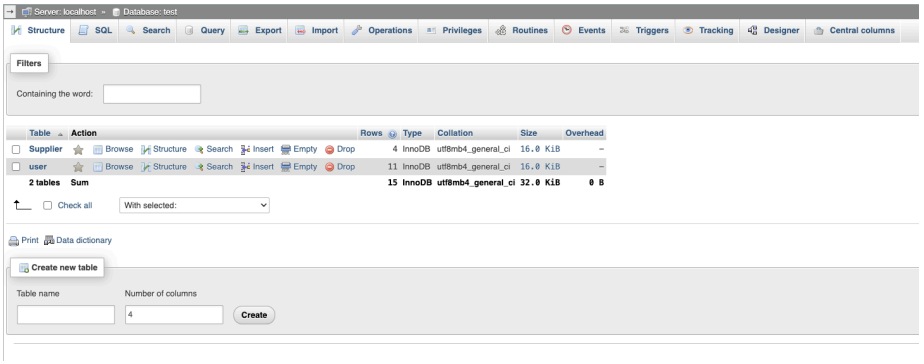


Figure 8.2: Compromised Database

Collection

During the collection phase of our forensic investigation into the cyber attack on 4GuysCoffee, our primary objective was to gather relevant logs and data from various sources to piece together the sequence of events and assess the extent of the damage caused by the attack. We targeted three main sources of information: the compromised database, email servers, and affected folders.

Compromised Database Logs:

Collecting logs from the compromised database, in this case, MariaDB, is crucial for understanding the nature of the SQL injection attack and its impact on the system. Database logs typically include records of database transactions, queries, and errors. By analysing these logs, we can identify the specific SQL commands executed by the attacker, the tables and data accessed or manipulated, and any anomalies or errors that occurred during the attack. To collect database logs, we can use database management tools or query the database directly to extract relevant information.

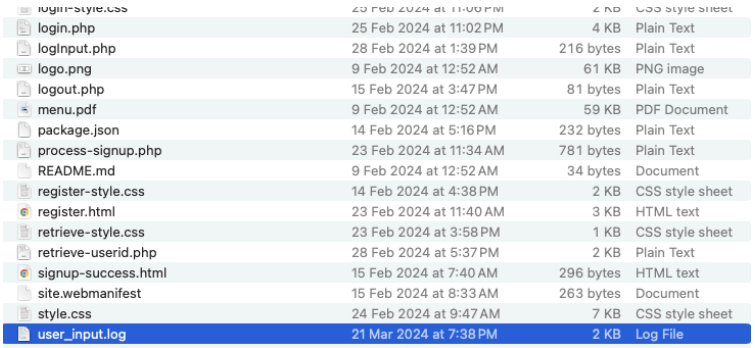


Figure 8.3: Folder containing Database Logs

Email Server Logs:
Gathering logs from the email servers is essential for tracing the origin and propagation of the malicious email used in the attack. Email logs contain records of email transactions, including sender and recipient addresses, timestamps, and message content. By analysing these logs, we can determine the source of the phishing email, track its distribution within the network, and identify any suspicious activities associated with compromised email accounts. We can access the server's administration console to collect email server logs or use email security tools that provide logging and monitoring functionalities.

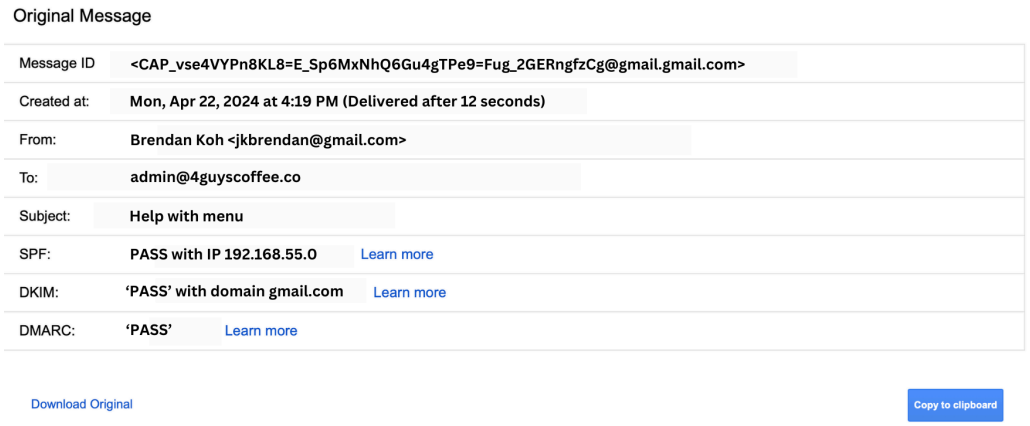


Figure 8.4: Email Logs

Affected Folders and File System Logs:
Examining logs from affected folders and the file system is crucial for understanding the attack's impact on critical files and data stored on the system. File system logs record file access, modification, deletion events and metadata such as file attributes and permissions. By analysing these logs, we can identify the files and folders targeted by the attacker, track changes made to the file system, and assess the extent of data loss or damage. To collect file system logs, we can use built-in logging mechanisms provided by the operating system or deploy file integrity monitoring tools that capture file system activities in real time.

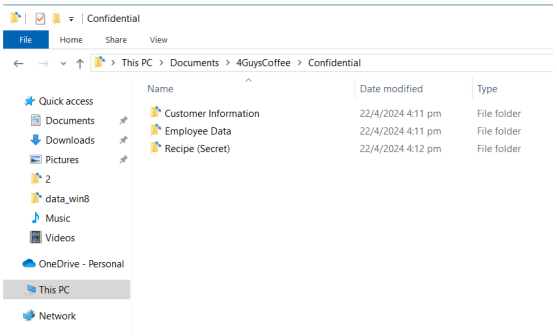


Figure 8.5: Compromised Folder

To collect data from these sources, we may need to work closely with system administrators and IT staff to gain access to the necessary systems and resources. It is essential to ensure that data collection procedures adhere to legal and regulatory requirements, such as obtaining proper authorisation and maintaining the integrity of the collected evidence.

Preservation

Preserving the integrity of digital evidence, especially in a forensic investigation, is crucial to ensure that the evidence remains untampered with and admissible in legal proceedings. In the case of the cyber attack on 4GuysCoffee, we took the necessary steps to preserve both the compromised database and the specific partition containing the affected folders.

Database Preservation:

We created a duplicate data image to preserve the compromised database, MariaDB. This process involves making an exact copy of the database files, including all tables, records, and metadata. The duplicate image is a forensic artefact that can be analysed without altering the original data. To create the duplicate image, we utilised specialised imaging software or command-line tools to replicate the database files while maintaining their integrity.

FTK Imager: This versatile tool was pivotal in our preservation efforts. With FTK Imager, we meticulously created forensic images of the compromised MariaDB database and the specific partition containing the affected folders. We ensured the resulting images were forensic by configuring imaging options and closely monitoring the process. FTK Imager's built-in checksum verification tools allowed us to verify the integrity of the generated images, providing confidence in preserving the original data.

Partition Preservation:

In addition to preserving the compromised database, we also took steps to preserve the specific partition containing the affected folders on the system's storage device. This partition likely contains critical files and data the attacker targeted during the cyber attack. Similar to the database preservation process, we created a duplicate image of the partition to safeguard the original data from any alterations. This involved using disk imaging software or command-line utilities to capture the entire contents of the partition, including file structures, attributes, and permissions.

dd (Command-Line Utility): Together with the FTK Imager, we utilised dd, a powerful command-line utility, to create bitwise copies of the digital evidence. By specifying input and output devices or partitions and configuring additional options such as block size and data verification, dd facilitated the creation of accurate copies of the compromised database and affected partition. This approach provided an additional layer of redundancy in our preservation efforts.

Write Blocker Implementation:

We employed a write blocker to enhance the preservation process further and prevent unauthorised modifications to the duplicated images. A write blocker is a hardware or software tool that prevents write access to the storage device, ensuring that no changes can be made to the duplicated images once created. Using a write blocker guarantees the integrity of the digital evidence and maintains its admissibility in legal proceedings.

Tableau Forensic Write Blockers: To safeguard against unauthorised modifications to digital evidence during imaging, we employed Tableau Forensic Write Blockers. These specialised hardware devices ensured that the original data remained unchanged throughout imaging. By connecting the source storage device or disk to the Tableau Write Blocker and enabling

write-blocking functionality, we preserved the integrity of the digital evidence, maintaining its admissibility in legal proceedings.

Examination:

During the examination phase of our forensic investigation into the cyber attack on 4GuysCoffee, our forensic team meticulously validated the duplication process's accuracy. This crucial step involved comparing the hash values of the duplicate image with those of the original copy of the compromised data. By doing so, we aimed to ensure that the forensic analysis would be conducted on a replica of the compromised data, preserving its integrity and reliability for investigative purposes.

To accomplish this task, we utilised cryptographic hash functions, such as MD5, SHA-1, or SHA-256, to generate unique hash values for the original data and the duplicate image. These hash values serve as digital fingerprints of the data, representing its unique content and structure. Any changes or alterations to the data, no matter how minor, would result in a different hash value.

Generate Hash Values: Firstly, we used forensic software tools or command-line utilities to generate hash values for the original data and the duplicate image. Each data set was individually hashed to produce its hash value, including the compromised database and affected folders.

Compare Hash Values: Next, we compared the hash values of the original data with those of the duplicate image. This comparison was typically performed using digital forensic software that provides built-in functionality for hash verification. Alternatively, we could use command-line utilities or scripting languages to automate the comparison process.

Verify Integrity: Upon comparing the hash values, we verified whether they matched or were identical. A match between the hash values indicated the duplication process was successful, and the duplicate image accurately represented the original data. Conversely, any discrepancies or differences in the hash values suggest potential duplication process or data integrity issues.

By rigorously comparing the hash values of the duplicate image with those of the original data, we ensured the accuracy and reliability of the duplication process. This validation step is crucial in maintaining the integrity of digital evidence and instilling confidence in the results of the forensic analysis conducted during the investigation.

Comparing the hash values of Database images:

```
brendan@Brendans-MacBook-Pro Documents % shasum -a 256 Database.txt
83d48f7de2f2b0748c8fbebf1684a5400495ab0831314240c9449097d27de5d3  Database.txt
brendan@Brendans-MacBook-Pro Documents % shasum -a 256 Database\ Copy.txt
83d48f7de2f2b0748c8fbebf1684a5400495ab0831314240c9449097d27de5d3  Database Copy.txt
brendan@Brendans-MacBook-Pro Documents %
```

Comparing the hash values of Partition images:

```
brendan@Brendans-MacBook-Pro Documents % shasum -a 256 Partition.ica
7c6c23e90cd75e0dc7058038e6f34ed692305b9059b2141895537142d59597c7  Partition.ica
brendan@Brendans-MacBook-Pro Documents % shasum -a 256 Partition\ copy.ica
7c6c23e90cd75e0dc7058038e6f34ed692305b9059b2141895537142d59597c7  Partition copy.ica
brendan@Brendans-MacBook-Pro Documents %
```

Analysis

During the forensic analysis phase of our investigation into the cyber attack on 4GuysCoffee, we leveraged Autopsy, a powerful open-source digital forensics platform, to examine the recovered files and uncover evidence related to the attacker's activities.

File Recovery and Examination:

In the file recovery and examination phase of our forensic investigation using Autopsy, we meticulously followed a systematic process to recover missing files and examine their contents for evidence related to the cyber attack on 4GuysCoffee.

Firstly, we launched Autopsy and initiated a new case tailored to our investigation. Within this case, we added the disk or disk image containing the files we needed to recover, ensuring that Autopsy had access to the relevant data for analysis.

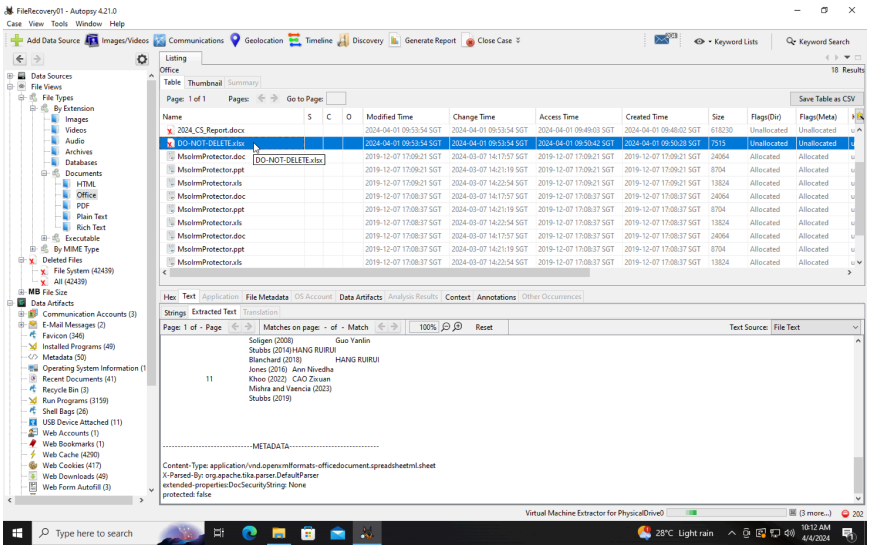
Next, we initiated the analysis process within Autopsy, allowing the software to scan the disk or image thoroughly. This scanning process generated a comprehensive list of files and other relevant data, providing us with a detailed overview of the contents of the disk or image.

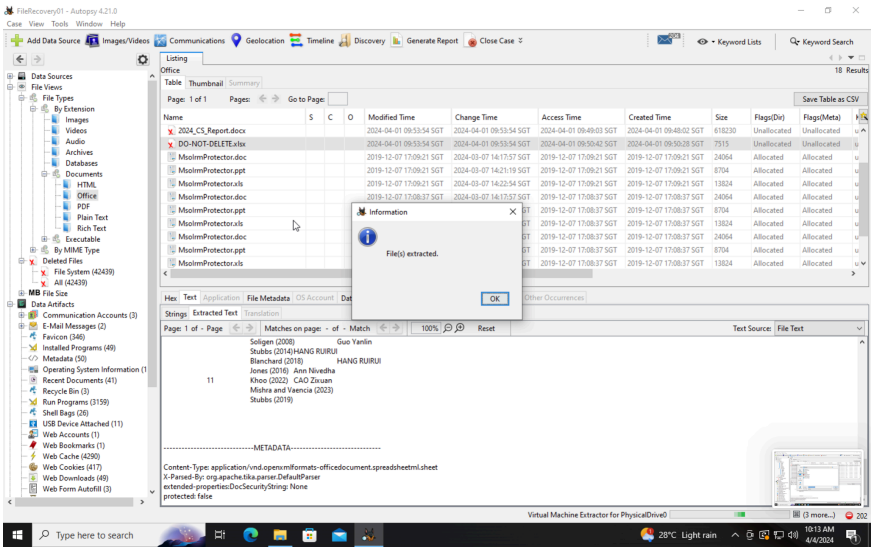
Once the analysis was complete, we utilised Autopsy's file browser to navigate to the directory where the 'confidential' folder containing the missing files was located. We employed Autopsy's search function within the 'confidential' folder to look for the missing files, namely 'DO-NOT-DELETE.xslx' and '2024_CS_Report.docx'.

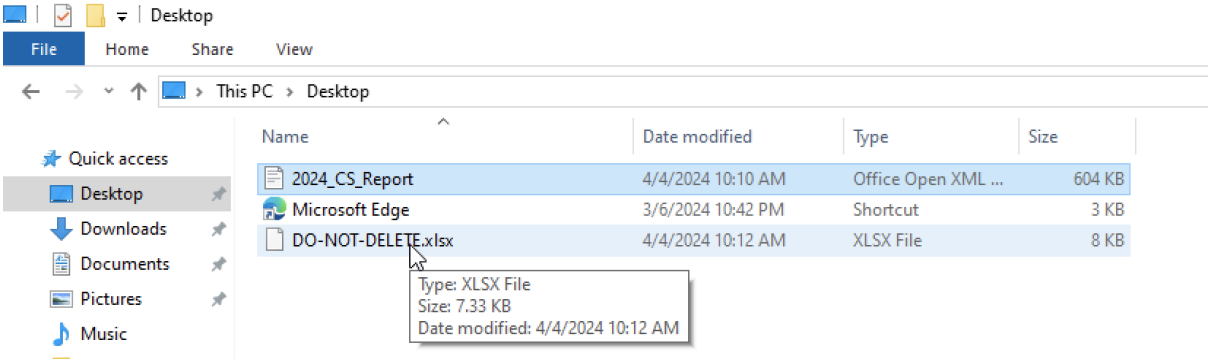
We selected the missing files for recovery after locating them within Autopsy's file browser. We specified a specific location on our system where we wanted the recovered files to be stored. Autopsy's intuitive interface facilitated this process, allowing us to recover the files easily.

Following the recovery process, we thoroughly examined the recovered files to ensure their integrity and accessibility. We verified that the recovered files were intact and could be opened without issues, confirming the successful recovery process.

By meticulously following these steps and utilising Autopsy's powerful recovery capabilities, we were able to recover the missing files related to the cyber attack on 4GuysCoffee. Autopsy's intuitive interface and comprehensive features were crucial in facilitating the file recovery, enabling us to retrieve valuable evidence for our forensic investigation.







Figures 8.6 - 8.8: File Recovery process

Log Analysis of Compromised DBMS:

In conducting a thorough database forensic analysis through log analysis, we employed specialised techniques to scrutinise the logs of events occurring within the Database

Management System (DBMS). By carefully examining these logs, we aimed to uncover evidence of the attacker's activities, mainly focusing on identifying SQL injection attempts and unauthorised access.

Firstly, we accessed the logs generated by the DBMS, which provide a detailed record of commands and queries executed within the database environment. These logs capture a range of activities, including user logins, queries executed, and modifications made to the database structure or content.

Our analysis focused on identifying anomalies and suspicious patterns within the logs, particularly indications of SQL injection attacks. SQL injection is a common attack vector wherein attackers exploit vulnerabilities in the input fields of web applications to inject malicious SQL commands into the database. By examining the syntax and structure of queries recorded in the logs, we looked for telltale signs of SQL injection attempts, such as unexpected characters or keywords commonly associated with injection attacks.

Additionally, we scrutinised the logs for evidence of unauthorised access or unusual activity within the DBMS. This included identifying logins from unfamiliar or suspicious IP addresses, distinctive patterns of query execution, or attempts to access sensitive data outside of normal usage patterns.

Furthermore, we traced the actions of specific user accounts within the logs to determine if the attacker had compromised or misused any accounts. By correlating user activity with known security incidents and patterns of malicious behaviour, we could pinpoint potential points of compromise and unauthorised access within the database environment.

```
2024-03-01 16:09:23: User input: " or ""="; #
2024-03-01 16:28:51: User input: 105; DROP TABLE Suppliers
2024-03-01 16:29:02: User input: 1; DROP TABLE Supplier
2024-03-01 16:32:10: User input: # DROP TABLE Supplier; #
2024-03-01 16:32:44: User input: /*! MYSQL special comment format */
2024-03-01 16:34:18: User input: SELECT * FROM Users WHERE Username = 'admin' AND '1'='1';
2024-03-01 16:34:33: User input: SELECT * FROM Users WHERE Username = 'admin' AND '1'='1'; #
2024-03-01 16:35:15: User input: SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME = 'Supplier';
2024-03-01 16:36:05: User input: ' OR '1'='1
2024-03-01 16:38:40: User input: ' UNION SELECT * FROM Suppliers --
2024-03-01 16:56:00: User input: ' UNION SELECT * FROM Supplier; #
2024-03-01 16:57:52: User input: SELECT * FROM Supplier;
2024-03-01 16:58:03: User input: s
2024-03-07 20:58:59: User input: ' OR 1=1 ; #
2024-03-09 14:14:50: User input: ' OR 1=1 UNION SELECT email, null, null FROM users --
2024-03-09 14:15:14: User input: ' OR 1=1
2024-03-09 14:15:38: User input: ' OR 1=1 UNION SELECT email, null, null FROM users -- ; #
2024-03-09 14:15:56: User input: ' OR 1=1 UNION SELECT email, null, null FROM test.users -- ; #
2024-03-09 14:16:10: User input: ' OR 1=1
2024-03-09 14:17:07: User input: ' OR 1=1 ; #
2024-03-09 14:39:49: User input: jkbrendan@gmail.com
2024-03-09 14:40:20: User input: jkbrendan@gmail.com
2024-03-09 14:41:34: User input: jkbrendan@gmail.com
2024-03-09 14:42:11: User input: ' OR 1=1
2024-03-09 14:42:24: User input: ' OR 1=1; #
2024-03-21 19:38:26: User input: ' OR 1=1 ; DROP TABLE Supplier; #
```

Figure 8.9: DB Logs showing SQLi

Examination of File Deletion Events:
In examining file deletion events as part of our forensic analysis, we employed meticulous techniques to scrutinise the logs and uncover evidence of the attacker's activities. We focused on identifying patterns and anomalies within the file system logs that could indicate malicious file deletion attempts to disrupt 4GuysCoffee's operations.

Firstly, we accessed the logs generated by the file system, which record various file-related events such as creation, modification, and deletion. These logs provide a chronological record of file system activity, including timestamps, user identifiers, and the actions performed on files and directories.

Our analysis concentrated on identifying file deletion events that deviated from standard usage patterns or were indicative of malicious intent. We looked for patterns such as bulk deletion of files or directories, deletion of critical system files, or deletion actions initiated from unauthorised user accounts.

Additionally, we examined the metadata associated with deleted files, including file attributes such as size, permissions, and timestamps. Discrepancies or inconsistencies in file attributes could indicate attempts by the attacker to conceal their actions or manipulate the file system for nefarious purposes.

Furthermore, we correlated file deletion events with other forensic evidence obtained during the investigation, such as network logs, system logs, and user activity records. This cross-referencing allowed us to establish a timeline of events and identify potential points of compromise or unauthorised access within the file system.

Email Analysis:
Our forensic analysis thoroughly examined email data to uncover evidence related to the attacker's activities. This involved scrutinising email server logs, message headers, and content to identify signs of unauthorised access, phishing attempts, and other malicious activities.

Firstly, we accessed the logs generated by the email server, which record a wealth of information, including sender and recipient addresses, timestamps, message content, and email routing information. These logs provide a detailed record of email transactions within the organisation's email system.

Our analysis focused on identifying abnormal email activities, such as suspicious login attempts, unusual message forwarding or redirection, and patterns indicative of phishing attacks. We looked for signs of unauthorised access to email accounts, including logins from unfamiliar IP addresses or devices and multiple failed login attempts.

Additionally, we examined email message headers to trace the origin and path of suspicious emails. By analysing the routing information in message headers, we identified potential sources of phishing emails and tracked their distribution within the organisation's email system.

Furthermore, we scrutinised the content of suspicious emails for signs of phishing attempts, including deceptive language, malicious attachments, and links to phishing websites. We also looked for evidence of email spoofing or impersonation, where attackers masquerade as legitimate senders to deceive recipients into disclosing sensitive information.

This comprehensive email data analysis uncovered evidence of the attacker's tactics and techniques, including attempts to gain unauthorised access to email accounts, distribute phishing emails, and deceive staff members. This forensic analysis provided valuable insights into the scope and impact of the cyber attack on 4GuysCoffee, enabling us to formulate effective strategies for response and mitigation.

```
From: Brendan Koh <jkbrendan@gmail.com>
Date: Mon, 22 Apr 2024 16:19:12 +0800
Message-ID:
<CAP_vse4VYPn8KL8=E_Sp6MxNhQ6Gu4gTPe9=Fug_2GERngfzCg@mail.gmail.com>
Subject: Fwd: Help with menu
To: "admin@4guyscoffee.co" <admin@4guyscoffee.co>
Content-Type: multipart/mixed; boundary="00000000000051b17c0616ab181c"

--00000000000051b17c0616ab181c
Content-Type: multipart/alternative; boundary="00000000000051b17a0616ab181a"

--00000000000051b17a0616ab181a
Content-Type: text/plain; charset="UTF-8"

Hello 4GuysCoffee admin,

I am Brendan, one of your customers. I haven't been to your cafe in some
time and was thinking of visiting soon. Can I double confirm if this is the
current menu?

Looking forward to hearing from you
Brendan

--00000000000051b17a0616ab181a
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
```

```
Delivered-To: admin@4guyscoffee.co
Received: by 2002:a05:6a06:98:b0:6c2:1fe8:6818 with SMTP id k24csp2110750pin;
        Mon, 22 Apr 2024 01:19:30 -0700 (PDT)
X-Received: by 2002:a05:690c:3685:b0:617:c9b0:e12c with SMTP id
fu5-20020a05690c368500b00617c9b0e12cmr8966339ywb.38.1713773964163;
        Mon, 22 Apr 2024 01:19:24 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1713773964; cv=none;
        d=google.com; s=arc-20160816;
        b=WSwRsZyQBOWxJ/1+8rVgRx70+mc0fu2jRP5tWLanWJaFCP/+NC+RCIqi0AREVmvlwu
         plSuGCCkymg4eanPEQ+tsUQ0XwUsLls47IdND7YWTYifmxvZKZh6+PjF1Rig/iSu4bNO
         n4yCqvZKGzJDKm0FgKJZ3B+DBwhpa0xf551EXr2IG0SE4N0S4JboZ+No/th5o+5vghQm
         F8sFVTdNMyMhecAY4Y9F+znijBNqaqj7jtmpcz5KlSY5aaHLq/p3Eihyd/vGJ2z/l2LY
         rVuop77LRTl7VU0EDznWQdpcdq6bFkQn5WSjIl5Sgsw3dvU3hyN8YWBAtk7IfCFXZ9Hr
         SK1Q==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=to:subject:message-id:date:from:in-reply-to:references:mime-version
         :dkim-signature;
        bh=5+r8w3bxDEL3JfSfhdN6rqdfrs90jUvPX7YEOema3n4=;
        fh=3g3GPrhHJlAbPMLEn5ERwlBt5BNTefOGPl0+wgOl/W4=;
        b=oGQETsiVHDc7+J+USFKPqFho/um7iHNKdouUYEiowS7oG6mKv0/191dA9W5HPX/XBE
         eZQqDlwxJycZ0gseJj9+50D2nh1edxvSPcu7SCPGZ2FRSOVWb+wwAji8BcTDD+w9Cw+q
         FabBa3ErzVS8ciLBkwOShRCH69G8qC8CjNifMqAzqXh6bkmS5DpcaSP4bVAj2x0Kih6Y
         TzwrwnBS9uUqW3vPrfaaOyMTxGlZ/g1SdAen7g56lcfSsRLv0FOxK5aord7IMtsc9PCe
         lfORSbKs07GDjX2xIBTlct3hBNspCUbsPyVtzKd0ov0hFmws27Ukp069Y3ZQb+Fz4iY7
         +Cfg==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20230601 header.b=iHwGdjLT;
       spf=pass (google.com: domain of jkbrendan@gmail.com designates 192.168.55.0 as permitted
sender) smtp.mailfrom=jkbrendan@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <jkbrendan@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [192.168.55.0])
        by mx.google.com with SMTPS id
```

Figure 8.10 - 8.11: Email Analysis

8. Cybersecurity GRC

Executive Summary

In today's dynamic business landscape, safeguarding information assets and ensuring regulatory compliance are paramount for organisational success. 4GuysCoffee recognises the importance of robust Information Security Governance, Risk, and Compliance (ISGRC) practices in managing risks effectively and fostering a culture of security awareness.

Our comprehensive ISGRC framework encompasses clear governance structures, rigorous risk management processes, and adherence to relevant laws and regulations. Through regular review and updates of our Business Continuity Plan (BCP) and Incident Response Process, we ensure resilience against many risks, including supply chain disruptions and cyber threats.

Critical systems such as our POS system, customer database, and financial records are protected through stringent security controls and regular vulnerability assessments. Leveraging Docker on AWS Linux on EC2 to host our SIEM system enhances security capabilities and reduces control costs.

Investing in employee education through interactive workshops, simulations, and online learning resources underscores our commitment to cultivating a security-conscious culture. By empowering employees with the knowledge and skills to identify and mitigate security risks, we fortify our defence against emerging threats.

Our overarching objective is to foster resilience against cyber threats while nurturing customer trust and confidence. By aligning our ISGRC practices with our strategic goals and embracing a proactive risk management and compliance approach, 4GuysCoffee is poised to navigate the evolving threat landscape with confidence and integrity.

Key Findings:

- Regular review and update of the Business Continuity Plan (BCP) to reflect changes in business operations and regulatory requirements
- The SysSP delineates crucial security controls aimed at safeguarding systems and software integrity.
- The Incident Response Process ensures timely identification and mitigation of security incidents, bolstering resilience against cyber threats.
- 4GuysCoffee confronts various risks, from supply chain disruptions to sophisticated cybersecurity threats.
- Critical systems and processes include POS systems, customer databases, financial records, and inventory management.
- Recovery Time Objectives (RTO) for critical systems are within 24 hours
- Identified vulnerabilities, such as unpatched bugs and weak web applications, underscore the necessity for proactive security measures.

- Predicted annual losses without security controls amount to S$11,990.00, significantly mitigated to a positive savings of S$6,757.00 post-control implementation, demonstrating the effectiveness of strategic investments.
- Leveraging Docker on AWS Linux EC2 to host SIEM reduces control costs and enhances security capabilities.
- Adopting a Learning Management System acknowledges the human element in cybersecurity and empowers employees through continuous education.
- The overarching objective is cultivating a security-conscious culture, fostering resilience against cyber threats and nurturing customer trust and confidence.

Introduction to Information Security Governance, Risk and Compliance

Definition

Information Security Governance, Risk, and Compliance (ISGRC) is a comprehensive framework 4GuysCoffee employs to manage and safeguard our information assets effectively. This framework encompasses several vital components. Firstly, Information Security Governance entails establishing clear policies, procedures, and structures to ensure that information security is effectively managed across the organisation. This involves defining the roles and responsibilities of individuals in the security program and setting strategic objectives aligned with the organisation's overall goals.

Secondly, Risk Management is a critical aspect of ISGRC. It involves identifying potential threats and vulnerabilities to the organisation's information assets, assessing the likelihood and potential impact of these risks, and implementing strategies to mitigate or manage them effectively. By systematically evaluating risks, organisations can prioritise their efforts and allocate resources more efficiently to protect against the most significant threats.

Lastly, Compliance is essential in ensuring that organisations adhere to relevant laws, regulations, and industry standards on information security. This includes data protection laws, industry-specific regulations, contractual obligations, and internal policies. Compliance efforts typically involve implementing controls and measures to meet these requirements and conducting regular audits and assessments to ensure ongoing adherence.

Importance of GRC

Governance, Risk, and Compliance (GRC) are essential for organisational success in today's business realm. GRC encompasses a holistic approach to managing risks by integrating governance structures, assessing risks, and ensuring compliance. This comprehensive strategy helps organisations identify, evaluate, and address potential risks before they escalate, safeguarding against potential disruptions and losses.

GRC is also crucial in aligning information security efforts with the organisation's strategic goals. By establishing clear governance frameworks and performance indicators, GRC

ensures that resources are efficiently allocated to support the organisation's mission while effectively managing risks.

Another significant aspect of GRC is ensuring compliance with laws, regulations, and industry standards. By staying updated on evolving compliance requirements, organisations can avoid legal penalties, regulatory fines, and damage to their reputation. GRC provides the necessary structure and guidance to navigate complex regulatory landscapes and demonstrate a commitment to ethical conduct and compliance.

Moreover, effective GRC practices improve decision-making by providing management with timely and relevant information on risk exposure and compliance status. This enables organisations to make informed decisions about risk management strategies, resource allocation, and strategic initiatives, ultimately leading to better outcomes and sustainable growth.

Investing in GRC initiatives can also lead to cost savings by preventing costly incidents such as data breaches and regulatory penalties. By proactively managing risks and ensuring compliance, organisations can mitigate such incidents' financial and reputational impacts, ultimately saving time and resources.

Lastly, GRC fosters a culture of continuous improvement by encouraging organisations to regularly assess, refine, and enhance their governance, risk management, and compliance practices. Embracing a proactive and iterative approach to GRC helps organisations adapt to changing threats and regulatory requirements, maintaining resilience and competitiveness in today's dynamic business environment.

Objectives of the report

This GRC report for 4GuysCoffee aims to evaluate and enhance the organisation's current GRC practices. The report seeks to assess the effectiveness of existing policies, procedures, and structures related to information security governance, risk mitigation, and compliance with laws and regulations. Additionally, it aims to identify any weaknesses or gaps in the organisation's GRC framework and provide actionable recommendations for improvement. The objective of strengthening governance structures, minimising risks, and ensuring compliance is to bolster 4GuysCoffee's overall security posture and promote continuous enhancement in GRC practices.

Organisational Profile

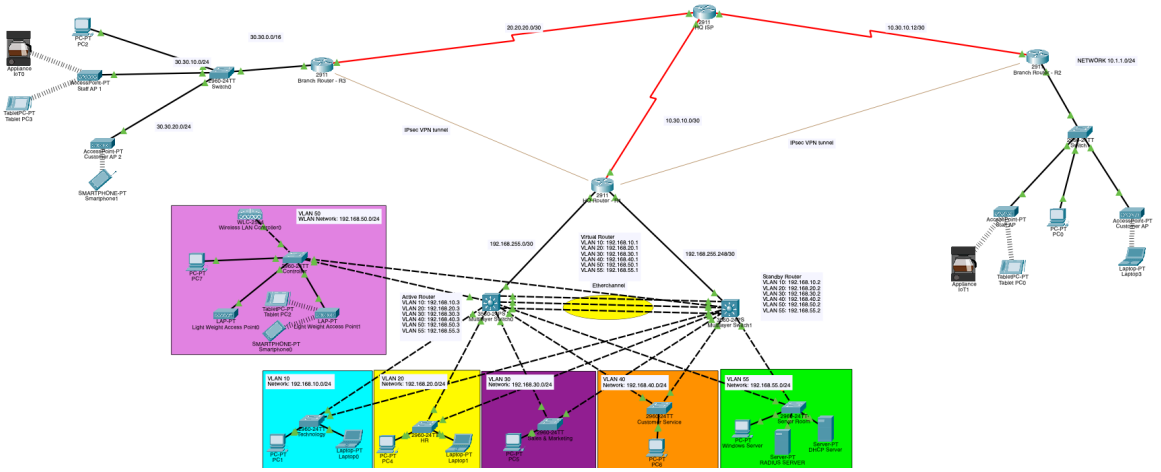
Description

4GuysCoffee, a thriving small and medium enterprise headquartered in Singapore, has made a significant mark in the competitive and dynamic coffee industry. Our commitment to delivering exceptional coffee experiences is evident in our focus on

using ethically sourced and sustainably grown beans, which are meticulously roasted and packaged in a local facility. This emphasis on sustainability aligns with the growing consumer demand for ethically sourced and environmentally friendly products in the global coffee market.

The company's cafes serve as more than just retail spaces; they are vibrant hubs that offer a diverse range of specialty coffees, providing customers with a unique and memorable coffee culture experience. Whether it is the aromatic blends, distinct brewing techniques, or the ambience of our cafes, 4GuysCoffee has carved a niche for itself in an industry where quality and innovation are paramount.

In addition to its physical presence, 4GuysCoffee has ventured into the digital realm by launching a global e-commerce store. This strategic move allows us to reach coffee enthusiasts worldwide, offering our signature roasted coffee beans for sale online. This expansion into e-commerce reflects the company's adaptability and recognition of evolving consumer preferences, especially when online shopping for speciality products has become increasingly popular.



At 4GuysCoffee, our network architecture follows a best-in-class approach, incorporating a three-tier hierarchical design for the headquarters and a simplified structure for branches. This widely acknowledged industry practice ensures reliability, scalability, and cost-effectiveness, optimising performance and enabling seamless scalability for future growth while maintaining efficient network management. The hierarchical design segregates functions clearly, enhancing overall reliability and robustness.

Our network infrastructure at the Distribution and Core Layer is designed for resilience. It includes a single HQ router supported by two multilayer switches for efficient inter-VLAN routing and redundancy through HSRP configuration. Implementing an EtherChannel between switches optimises bandwidth and load

balancing, significantly enhancing overall performance. Concurrently, using subnets and VLANs in conjunction forms a multilayer security approach, effectively addressing Layers 2 and 3 vulnerabilities.

To future-proof the network for business expansion, subnet selection adheres to Cisco's guidelines on Variable Length Subnet Masking (VLSM), allocating space for growth with */16* and */24* for the HQ and different departments, ensuring scalability. Layer 2 security measures such as PortFast, BPDUguard, port security, and auto-trunking disabling are prioritised to fortify against potential threats.

Routing is accomplished through OSPF, which was chosen for its compatibility with diverse networks compared to the limited scope of EIGRP. For Wireless Local Area Network (WLAN) security, RADIUS server authentication enhances access control with unique username and password combinations. IPSec VPNs are deployed for secure site-to-site connections, guaranteeing data integrity and confidentiality.

Structure and Hierarchy

At 4GuysCoffee, we uphold a structured organisational hierarchy to efficiently manage our operations and ensure clarity in roles and responsibilities. Our organisational structure encompasses various departments spearheaded by experienced professionals overseeing specific business aspects.

1. Reporting Structure:

General Manager (GM): Directly oversees all departments.

Department Heads:
Technology: Head of Department reports to the GM. 3 employees report to the Head of Technology (HOT).
HR: Head of Department reports to the GM. 2 employees report to the Head of HR (HOHR).
Customer Service: The head of the department reports to the GM. 2 employees report to the Head of Customer Service (HOCS).
Sales & Marketing: The head of the department reports to the GM. 9 employees report to the Head of Sales & Marketing (HOSM).
Logistics: The head of department reports to the GM. 9 employees report to the Head of Logistics (HOL).
Roasting Facility: The head of the department reports to the GM . 9 employees report to the Head of Operations (HOO).

Cafe Staff: Report to their respective Branch Managers (BM). The respective BMs will report to the HOO, who will report directly to the GM.
A total of 114 employees are distributed across 6 outlets:
Century Square, Tampines: 19 employees report to the Tampines BM.
Paragon, Orchard: 19 employees report to the Orchard BM.
Jewel, Changi Airport: 19 employees report to the Jewel BM.
JEM, Jurong East: 19 employees report to the Jurong East BM.
Resorts World, Sentosa: 19 employees report to the Sentosa BM.
Singpost Center, Paya Lebar: 19 employees report to the Singpost Center BM.

2. Employee Breakdown:
Total employees in Singapore: 161
Technology: 3 employees
HR: 2 employees
Customer Service: 2 employees
Sales & Marketing Ecom: 9 employees
Logistics: 9 employees
Roasting Facility: 9 employees
Cafe Staff: 114 employees (distributed across 6 outlets)
Branch Managers: 6 employees

Overview of Operations

At 4GuysCoffee, we meticulously shape our operations to offer coffee and outstanding experiences grounded in sustainability, innovation, and operational excellence. We start by carefully selecting ethically and sustainably grown coffee beans from various countries worldwide, ensuring fair trade and eco-friendly practices through direct relationships with farmers. Once acquired, these top-quality beans undergo careful roasting in our advanced facility in Singapore. Our skilled roasting team uses precise methods to bring out the full flavour of each bean while maintaining consistency across our products. Rigorous quality checks at every stage ensure that only the best coffee reaches our customers, reflecting our unwavering dedication to delivering unmatched taste and freshness.

Apart from roasting, our cafe outlets provide vibrant spaces where customers can enjoy a diverse selection of specialty coffees and immerse themselves in our unique coffee culture. Each outlet is designed to create a warm and inviting atmosphere, with knowledgeable staff dedicated to exceptional service. Our cafe managers oversee day-to-day operations to ensure every customer has a memorable and satisfying experience, whether enjoying their favourite brew or trying new flavours.

In response to the changing preferences of consumers, we've launched a global e-commerce store to extend our reach beyond physical locations. This platform allows coffee enthusiasts worldwide to access our signature beans easily, strengthening our brand presence and engaging with a broader customer base through digital marketing and efficient order processing.

At the core of our operations is a relentless pursuit of efficiency and innovation. We use advanced technology and strategic partnerships to optimise supply chain management, inventory control, and customer service processes. Our commitment to innovation extends to product development, where we explore new brewing methods, flavours, and packaging to stay ahead in the competitive coffee industry.

4GuysCoffee is more than just a coffee company; it's a testament to our dedication to delivering exceptional experiences. From sourcing to serving, every aspect of our operations reflects our commitment to quality, sustainability, and customer satisfaction, ensuring that each cup of coffee tells a story of craftsmanship, care, and excellence.

Regulatory and Compliance Landscape

Applicable regulations and standards

Data Protection Laws: Ensuring compliance with data protection laws, notably the General Data Protection Regulation (GDPR) in Europe and the Personal Data Protection Act (PDPA) in Singapore, is paramount for 4GuysCoffee, especially concerning the operation of our online store that ships internationally. These regulations govern customer data collection, processing, and storage, requiring us to implement stringent measures to handle personal information securely. Under GDPR and PDPA, we are obligated to obtain explicit consent from customers before collecting their data, clearly communicate how their information will be used, and ensure that it is handled confidentially and in accordance with their preferences. Additionally, we must provide customers the option to access, update, or delete their data upon request, as mandated by these regulations.

Payment Card Industry Data Security Standard (PCI DSS): Compliance with PCI DSS is essential for securely processing, storing, and transmitting credit card information to prevent data breaches and protect cardholder data. Compliance with PCI DSS is indispensable for our online transactions, mainly when processing credit card payments. As we collect and process payment information from customers worldwide, adhering to PCI DSS standards is essential to safeguarding sensitive cardholder data and preventing breaches. To comply with PCI DSS requirements, we employ encryption methods to protect payment data during transmission, maintain secure networks and systems to prevent unauthorised access, and regularly conduct security assessments and audits to ensure ongoing compliance. Additionally, we

implement strict access controls and authentication measures to restrict access to payment information only to authorised personnel.

Food Safety Regulations: Adhering to food safety regulations is of utmost importance for 4GuysCoffee in Singapore, where stringent measures are in place to ensure the quality and safety of food products served in our cafe outlets. Singapore has a comprehensive regulatory framework overseen by the Singapore Food Agency (SFA) to uphold food safety standards and protect public health.

In accordance with Singapore's food safety regulations, our cafe outlets follow strict protocols for food handling, storage, and preparation to minimise the risk of contamination and foodborne illnesses. This includes regular training and certification of our staff in proper hygiene practices, such as handwashing, sanitisation of utensils and surfaces, and safe food handling techniques.

Moreover, our cafe outlets adhere to specific guidelines for storing perishable ingredients, ensuring that temperature controls are maintained to prevent spoilage and bacterial growth. This involves regular monitoring of refrigeration units and storage areas to ensure food items are stored at optimal temperatures to preserve freshness and quality.

Regarding food preparation, our cafe outlets strictly adhere to standardised recipes and cooking procedures to maintain consistency and ensure food is prepared safely and hygienically. This includes measures to prevent cross-contamination, such as separate cutting boards and utensils for raw and cooked foods and proper cooking temperatures to eliminate harmful bacteria.

Additionally, our cafe outlets undergo regular inspections by the SFA to ensure compliance with food safety regulations. These inspections cover various aspects, including cleanliness of premises, food storage practices, hygiene standards of staff, and adherence to food handling protocols. Any deviations from regulatory requirements are promptly addressed and rectified to maintain compliance and uphold our commitment to food safety and customer well-being.

Our vacuum-sealed coffee beans typically maintain quality for about a year when unopened and up to a month once opened. We have implemented stringent measures to ensure adherence to expiration dates, particularly in light of recent incidents in Singapore where the SLA fined companies for tampering with expiration dates.

Adherence to food safety regulations in Singapore is non-negotiable for 4GuysCoffee, as we prioritise the health and safety of our customers by ensuring that our cafe outlets consistently meet the highest standards of food hygiene and quality.

Employment Laws: Compliance with employment laws in Singapore is fundamental for 4GuysCoffee to ensure fair and lawful treatment of our employees. Singapore maintains robust labour laws overseen by the Ministry of Manpower (MOM), aimed at safeguarding the rights and welfare of workers across various industries.

Central to employment laws in Singapore is the adherence to minimum wage requirements, which establish a baseline level of compensation for workers. While Singapore does not have a statutory minimum wage, the government sets guidelines and recommendations through the Tripartite Cluster for Cleaners (TCC) and the Progressive Wage Model (PWM) for specific sectors to ensure fair wages for low-wage workers.

Moreover, compliance with regulations governing working hours is essential to prevent exploitation and ensure work-life balance for employees. The Employment Act in Singapore stipulates standard working hours, overtime pay rates, and mandatory rest days for employees, providing legal safeguards against excessive working hours and ensuring adequate rest periods.

Additionally, Singapore's employment laws encompass a comprehensive framework of employee rights, including protection against unfair dismissal, discrimination, and harassment in the workplace. The Employment Act establishes basic entitlements such as annual leave, sick leave, and public holiday entitlements. At the same time, the Workplace Safety and Health Act (WSHA) ensures a safe and conducive work environment for all employees.

Furthermore, Singapore employers must adhere to employee benefits and entitlements regulations, such as Central Provident Fund (CPF) contributions, medical insurance coverage, and employee compensation schemes. These provisions promote employee well-being and financial security, fostering a conducive work environment that attracts and retains talent.

Compliance with employment laws in Singapore is integral to 4GuysCoffee's commitment to upholding fair labour practices and ensuring the welfare and rights of our employees. By adhering to minimum wage requirements, regulating working hours, and safeguarding employee rights, we demonstrate our dedication to fostering a supportive and equitable workplace culture that contributes to our business's overall success and sustainability.

Environmental Regulations: Compliance with environmental regulations in Singapore is paramount for 4GuysCoffee to minimise our environmental footprint and promote sustainable business practices. Singapore has stringent environmental laws and regulations overseen by the National Environment Agency (NEA) and the Ministry of

Sustainability and the Environment (MSE) to safeguard the country's environment and natural resources.

One key aspect of environmental regulations in Singapore is waste management. As a food and beverage establishment, 4GuysCoffee must comply with laws governing waste disposal, recycling, and treatment. This includes appropriately segregating waste streams, such as food waste, recyclables, and general waste, to facilitate recycling and minimise landfill disposal. Additionally, we must engage licensed waste collectors and disposers to ensure that waste is managed responsibly and in compliance with environmental standards. Furthermore, compliance with environmental regulations extends to energy consumption and efficiency. Singapore encourages businesses to adopt energy-efficient practices and technologies to reduce energy consumption and greenhouse gas emissions. This involves investing in energy-efficient appliances and equipment, implementing energy-saving lighting systems, and optimising HVAC systems to minimise energy wastage. 4GuysCoffee can lower operational costs and contribute to Singapore's sustainability goals by adhering to energy efficiency guidelines.

In addition to waste management and energy efficiency, compliance with environmental regulations also encompasses sustainability practices. This includes initiatives to reduce single-use plastics, promote reusable and biodegradable packaging, and minimise water usage. 4GuysCoffee can implement measures such as offering incentives for customers to bring their reusable cups, sourcing sustainable and eco-friendly packaging materials, and implementing water-saving measures in our cafe operations. By prioritising sustainability, we reduce our environmental impact and contribute to building a greener and more sustainable future for Singapore.

Compliance with environmental regulations in Singapore is essential for 4GuysCoffee to demonstrate our commitment to environmental stewardship and responsible business practices. By adhering to waste management protocols, optimising energy usage, and promoting sustainability initiatives, we can minimise our environmental footprint and contribute to Singapore's efforts towards a cleaner and more sustainable environment.

Compliance requirements and challenges

Due to our international online store operations, ensuring compliance with data protection laws, such as the GDPR in Europe and the PDPA in Singapore, is crucial for 4GuysCoffee. These regulations demand strict measures for collecting, processing, and securely storing customer data. Obtain explicit consent from customers before data collection and allow them options to manage their data in a

way that aligns with these rules. However, implementing these measures consistently across diverse regions and keeping up with evolving regulations require work.

Similarly, meeting PCI DSS standards is vital for securely processing credit card information in our online transactions. Encrypting payment data during transmission, maintaining secure networks, and regular security assessments are crucial. Yet, ensuring compliance across various platforms and gateways and mitigating data breach risks remain challenging.

Adhering to food safety regulations in Singapore is essential for maintaining the quality and safety of our cafe's food products. Training staff in proper hygiene practices, following strict storage and preparation guidelines, and addressing regulatory deviations are critical but challenging tasks.

Compliance with employment laws, including minimum wage requirements and employee rights protection, is integral to the fair treatment of our employees. Navigating complex labour laws, managing payroll and benefits compliantly, and resolving employee grievances present ongoing challenges.

Lastly, adhering to environmental regulations is vital for reducing our environmental impact. Implementing effective waste management, optimising energy usage, and sourcing sustainable materials pose challenges while balancing cost-effectiveness and operational efficiency.

Information Security Governance Framework

Description of governance framework in place

At 4GuysCoffee, we have established a robust Information Security Governance Framework to ensure our critical information assets' confidentiality, integrity, and availability. This framework is a strategic roadmap for managing and mitigating organisational information security risks.

Our Information Security Governance Framework is designed to provide a structured approach to managing information security risks in alignment with industry best practices and regulatory requirements. It encompasses a set of policies, procedures, and controls to safeguard our information assets from unauthorised access, disclosure, alteration, and destruction.

Roles and responsibilities of key stakeholders

General Manager (GM):

As the highest-ranking executive in the organisation, the General Manager (GM) holds overarching responsibility for the governance, risk management, and compliance (GRC) efforts. He ensures robust GRC policies and procedures are established, effectively communicated, and consistently enforced throughout the organisation. This includes overseeing the implementation of risk management

strategies and initiatives to align with the organisation's business objectives. Regularly reviewing GRC performance metrics and reporting to the executive leadership team and the board of directors are also integral to the GM's role, ensuring transparency and accountability in GRC practices.

Department Heads:

Technology:

The Head of Technology (HOT) collaborates closely with the GM to develop and implement technology-related GRC policies and procedures. This involves ensuring that information systems and technology infrastructure comply with relevant regulatory requirements and industry standards. Additionally, the HOT is responsible for managing risks associated with technology systems and implementing controls to mitigate vulnerabilities effectively. By staying abreast of emerging threats and technological advancements, they contribute to the organisation's overall resilience against cyber threats and ensure the confidentiality, integrity, and availability of critical data and systems.

Human Resources:

The Head of HR (HOHR) plays a pivotal role in establishing and maintaining HR policies and procedures that comply with employment laws and regulations. He oversees employee-related risks, including those related to labour laws and employee rights, and implements measures to mitigate them effectively. Providing ongoing employee training and support on compliance matters, such as data protection and privacy, is also within his purview. By fostering a culture of compliance and ethical conduct within the organisation, the HOHR contributes to a positive and supportive work environment where employees feel valued and respected.

Customer Service:

The Head of Customer Service (HOCS) is responsible for implementing policies and procedures that ensure compliance with customer service regulations and standards. This includes managing risks associated with customer interactions and ensuring that customer data is handled securely and complies with relevant laws. By monitoring customer feedback and complaints, the HOCS identifies opportunities for improvement in service delivery and ensures that customer expectations are met or exceeded consistently. His role is crucial in maintaining high levels of customer satisfaction and loyalty, which are essential for the organisation's success and reputation.

Sales and Marketing:

The Head of Sales & Marketing (HOSM) is tasked with developing and enforcing policies and procedures related to marketing and sales practices, ensuring compliance with relevant regulations. This involves managing marketing campaigns, promotions, and advertising risks to protect the organisation's reputation and integrity. By collaborating with legal and compliance teams to review marketing materials for

compliance, the HOSM helps mitigate legal and regulatory risks while maximising the effectiveness of marketing initiatives. Their strategic approach to compliance ensures that sales and marketing efforts are aligned with the organisation's values and objectives, contributing to sustainable growth and success.

Logistics:

The Head of Logistics (HOL) oversees developing and maintaining policies and procedures for supply chain management and logistics operations. Their role involves identifying and mitigating risks related to supply chain disruptions, vendor relationships, and transportation logistics to ensure business continuity and operational efficiency. Ensuring compliance with regulations governing import/export, transportation, and warehousing activities is a key aspect of their responsibilities. By implementing robust controls and monitoring mechanisms, the HOL safeguards the integrity and security of the organisation's supply chain, fostering trust and reliability among stakeholders.

Roasting Facility and Cafe Operations:

The Head of Operations (HOO) establishes and enforces GRC policies and procedures for the roasting facility and cafe operations. This includes ensuring compliance with food safety regulations and industry standards to maintain product quality, safety, and integrity throughout the roasting process. Managing risks associated with food handling, storage, and preparation processes is critical to their role. The HOO contributes to the organisation's commitment to delivering high-quality products that meet regulatory requirements and customer expectations by implementing controls and best practices in food safety and hygiene.

Risk Management

Risk Assessment Methodology

Risk Management at 4GuysCoffee involves a structured approach to identify, assess, and mitigate potential risks that may impact our operations, reputation, and objectives. We utilise the NIST risk assessment methodology as much as possible to systematically evaluate risks across different areas of the organisation.

Qualitative Risk Assessment: This method involves a subjective evaluation of risks based on criteria such as likelihood and impact. By considering factors such as the probability of occurrence and the potential impact on business objectives, we can prioritise risks and identify areas that require immediate attention. Qualitative risk assessment allows us to take a broad view of risks, considering their qualitative aspects without assigning numerical values. This approach enables us to identify emerging risks, vulnerabilities, and areas for improvement across various aspects of our operations, including supply chain management, cybersecurity, regulatory compliance, and market competition.

Step 1: Identify Risks:
At 4GuysCoffee, our qualitative risk analysis process begins with identifying potential risks. We encourage team members to contribute their insights and observations, fostering a collaborative approach to risk identification. Brainstorming sessions and discussions help us create a comprehensive master list of risks, considering various aspects of our operations and potential vulnerabilities.

Step 2: Classify Risks:
Next, we classify risks using techniques such as the risk matrix. This method combines the consequences and likelihood of each risk occurring, providing a structured approach to prioritising risks. Additionally, we assess each risk's possible causes and effects and prepare for different scenarios, ensuring a holistic understanding of potential impacts.

Step 3: Control Risks:
Risk control involves targeting the root causes of risks and lessening their negative impact. We address hazards and inefficient processes to mitigate risks at their source while implementing corrective actions to minimise consequences. Providing workers with Personal Protective Equipment (PPE) and implementing safety protocols are examples of risk control measures we employ.

Step 4: Monitor Business Risks:
Throughout the qualitative risk analysis process, we maintain detailed records of identified risks, their ratings, and control measures. This information is essential for ongoing risk monitoring, where we observe the effectiveness of risk control measures and assess whether risks have been correctly classified. Continuous monitoring ensures that our risk management strategies remain effective and adaptable to changing circumstances.

Quantitative Risk Assessment: Quantitative risk assessment involves assigning numerical values to risks, such as probabilities and financial impacts, to quantify their potential consequences accurately. This method lets us prioritise risks based on their estimated likelihood and magnitude, facilitating more informed decision-making.

Step 1: Identify the Purpose, Scope, Method
Project managers define the purpose and scope of the quantitative risk analysis, outlining what insights they seek to gain and the limitations of the analysis. They select an appropriate method, such as Failure Mode and Effects Analysis (FMEA), Business Impact Analysis (BIA), or Expected Monetary Value (EMV) based on the specific objectives.

Step 2: Prepare the Data, Tools, and People Needed

Data relevant to the analysis and the necessary tools and resources are organised and prepared. This may involve gathering financial data, utilising specialised software, and involving relevant stakeholders or experts. Data accuracy and compatibility with the chosen method are crucial for accurate analysis.

Step 3: Apply the Chosen Method to the Data Gathered

The selected method is applied to the prepared data to assess risks and their potential impacts quantitatively. Techniques such as FMEA and BIA utilise predefined templates, while EMV calculations determine the expected monetary value of each risk based on probability and impact.

Step 4: Record and Store All Results

Results from the quantitative analysis are recorded and securely stored for future reference. This information provides valuable insights for future risk assessments and helps track changes in risk profiles over time. Keeping comprehensive records ensures that the effort invested in quantitative analysis is maximised and effectively informs future risk management strategies.

Identified Risks and Potential Impact

At 4GuysCoffee, we face diverse risks inside and outside our business. Changes in consumer tastes, tough competition, and economic ups and downs are major external risks. Dependence on suppliers for coffee beans can lead to shortages or quality problems. Internally, issues like inventory mismanagement or outdated systems can slow us down. Compliance with regulations and cybersecurity threats add further challenges. To stay strong, we need proactive strategies to handle these risks and keep our business running smoothly.

Supply Chain Disruptions: Supply chain disruptions present a considerable risk to 4GuysCoffee's operations, particularly concerning the sourcing of coffee beans and logistical challenges in transportation. Delays in procuring high-quality coffee beans from our suppliers can impact our ability to meet customer demand and maintain the freshness and quality of our products. Additionally, logistical challenges, such as disruptions in transportation routes or delays in delivery schedules, can further exacerbate these issues, leading to potential stock shortages and customer dissatisfaction.

Cybersecurity Threats: As our business increasingly relies on digital technologies and online platforms for various operations, cybersecurity threats pose a significant risk to the security and integrity of our sensitive information and customer data. Common cybersecurity threats, such as data breaches, phishing attacks, and ransomware

incidents, can result in unauthorised access to confidential data, financial losses, reputational damage, and legal liabilities.

Regulatory Compliance: Maintaining compliance with regulatory requirements is critical for 4GuysCoffee to operate legally and ethically while avoiding penalties and reputational damage. Changes in regulatory frameworks, such as data protection laws (e.g., GDPR, PDPA) and food safety regulations, necessitate continuous monitoring and adaptation of our policies and procedures to remain compliant. Non-compliance with these regulations can result in significant financial penalties, legal consequences, and loss of trust among customers and stakeholders.

Market Competition: The coffee industry is highly competitive, with numerous players vying for market share and consumer attention. Intense competition risks 4GuysCoffee's profitability and sustainability, necessitating strategic initiatives to differentiate our products, enhance customer experience, and stay ahead of competitors. Market competition can lead to price wars, erosion of profit margins, and challenges in attracting and retaining customers.

Risk Treatment Strategies

Risk Avoidance: When risks present significant threats to our organisation, we may avoid or eliminate them by discontinuing certain activities or refraining from engaging in high-risk ventures. For instance, if a particular supplier consistently poses a high risk of supply chain disruptions, we may terminate our relationship with them to mitigate the risk of stock shortages and customer dissatisfaction. In response to the identified risk of potential supply chain disruptions due to reliance on a single coffee bean supplier, we have decided to diversify our supplier base by engaging with multiple suppliers across different regions. This strategy reduces the likelihood of disruptions caused by transportation delays, quality issues, or unforeseen events affecting a single supplier's operations.

Risk Mitigation: Involves implementing proactive measures to reduce the likelihood or impact of identified risks. This approach may include implementing robust cybersecurity controls, such as firewalls and encryption protocols, to protect sensitive information from data breaches and cyber-attacks. To address the cybersecurity threat identified, 4GuysCoffee implements comprehensive cybersecurity measures, including regular software updates, employee training on cybersecurity best practices, and deploying intrusion detection systems. We also conduct security assessments and vulnerability scans to proactively identify and address potential weaknesses. By investing in robust cybersecurity measures, 4GuysCoffee mitigates the risk of data breaches, cyber-attacks, and unauthorised access to sensitive information.

Risk Transfer: Involves transferring the financial consequences of risks to third parties through insurance coverage or contractual agreements. By transferring the responsibility for managing specific risks to external parties, such as insurance

providers, we can mitigate the financial impact of unforeseen events while maintaining continuity in our business operations. For example, we may invest in cyber insurance to offset the costs associated with data breaches and cyber incidents. Given the potential financial impact of supply chain disruptions, 4GuysCoffee transfers this risk through contractual agreements with suppliers. The company negotiates service-level contracts that include clauses for compensation in the event of disruptions beyond the supplier's control. By transferring the financial responsibility for disruptions to its suppliers, 4GuysCoffee mitigates the risk of revenue loss and operational disruptions.

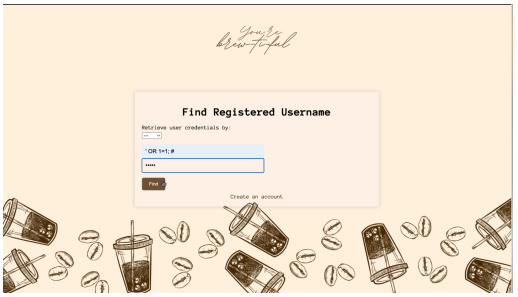
Risk Acceptance: Involves accepting risks deemed acceptable due to their minimal potential impact or the disproportionate cost of mitigation. This approach involves carefully assessing risk-reward trade-offs and determining whether the benefits of accepting the risk outweigh the potential consequences. For instance, if the cost of implementing additional security measures exceeds potential losses, we may accept the risk and allocate resources to address more significant threats. Despite the competitive nature of the coffee industry, 4GuysCoffee accepts the risk of market competition and focuses on differentiating its products and enhancing customer experience. The company invests in innovative offerings, sustainable sourcing practices, and personalised customer service to distinguish itself from competitors. While acknowledging market challenges, 4GuysCoffee remains confident in its ability to adapt and maintain its preferred choice among customers.

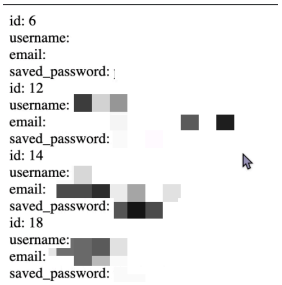
Overview of potential threats

It is crucial to highlight 4GuysCoffee's vulnerability to cyber threats due to our extensive reliance on technology for daily operations. As a cafe company with islandwide operations, our network infrastructure, web servers, and databases are all potential targets for cyberattacks. These threats pose a significant risk of disruption and financial loss, underscoring the importance of robust cybersecurity measures to safeguard our business operations and customer data.

Cyber-attacks:

In the past, 4GuysCoffee experienced firsthand the detrimental impact of cyberattacks when our website fell victim to a SQL injection attack. This attack targeted a vulnerability in our username retrieval page, exploiting it to gain unauthorised access to our website's database. As a result, sensitive customer information stored within the database, such as usernames and passwords, was compromised. This incident threatened our customers' privacy and security and caused reputational damage to our brand. It underscored the urgent need for enhanced cybersecurity measures to prevent future attacks and protect our businesses and customers from malicious activities.





Figures 9.1 - 9.2: SQLi attack on 4GuysCoffee

The incident underscores the perpetual requirement for vigilance and proactive security measures within 4GuysCoffee. Cyber attacks like SQL injection breaches and insider threats stemming from employees or contractors who have access to sensitive information significantly jeopardise data security. For instance, there have been instances within our organisation where employees were unwittingly deceived into opening seemingly innocuous PDF files containing malicious reverse shells. These shells facilitated unauthorised access to our systems, resulting in the deletion of crucial files and disruptions to our operations. These occurrences emphasise the critical necessity of cybersecurity awareness training for all employees to bolster our defences against evolving cyber threats and mitigate the potential risks associated with insider attacks.

Beyond Traditional Threats:

The expanding interconnectedness of our business introduces a host of additional security risks, particularly concerning our global sourcing of coffee beans and reliance on roasting facilities. With our extensive supply chain spanning multiple regions, these external partnerships present potential vulnerabilities. A report published in the first quarter of 2024 analysing entities in the United States revealed that in 2023 alone, at least 2769 entities fell victim to supply chain cyber-attacks. This alarming statistic underscores the pervasive nature of supply chain vulnerabilities across industries. Weaknesses in the cybersecurity practices of our third-party vendors, suppliers, or partners could be exploited by malicious actors to gain unauthorised access to our systems or sensitive data. For instance, a compromised vendor system could serve as a launching pad for infiltrating our infrastructure,

posing significant risks to the integrity and security of our operations. As such, we must implement stringent security measures and conduct thorough assessments of our supply chain partners to mitigate the potential impact of supply chain cyber-attacks and safeguard our organisation against external threats.

Mitigating the Risks:

To effectively combat the evolving cyber threats facing 4GuysCoffee, it's imperative to establish a comprehensive cybersecurity strategy. This strategy should encompass several key components:

- Regular Software Updates: Regularly updating software and firmware on all devices is essential to patch known vulnerabilities and mitigate the risk of exploitation by cyber attackers. As highlighted earlier, the reverse shell attack was mainly due to the PDF reader not being updated to the latest version that has already addressed the reported vulnerability (CVE-2023-26369). Ensuring that all software is kept up-to-date with the latest security patches can minimise the likelihood of similar incidents occurring in the future.
- Robust Network Security Measures: Implementing robust network security measures such as firewalls and Intrusion Detection Systems (IDS) is crucial for safeguarding our network infrastructure from unauthorised access and malicious activities. Firewalls are a barrier between our internal network and external threats, while IDS continuously monitors network traffic for suspicious behaviour and potential security breaches.
- Data Encryption: Employing data encryption for sensitive information at rest and in transit helps protect against unauthorised access and data breaches. By encrypting sensitive data, such as customer information and financial records, we can ensure that even if it falls into the wrong hands, it remains unintelligible and unusable.
- Cybersecurity Awareness Training: Providing ongoing cybersecurity awareness training for employees is essential to empower them to identify and avoid common cyber threats, such as phishing attempts. Educating employees on recognising suspicious emails, links, and attachments can significantly reduce the risk of falling victim to cyber-attacks and accidental data breaches.
- Regular Security Assessments: Regular security assessments, including vulnerability scans and penetration testing, are vital for identifying and addressing potential weaknesses in our systems and supply chain. By proactively assessing our security posture, we can identify vulnerabilities before they can be exploited by cyber attackers and take corrective action to mitigate risks.

By implementing these proactive cybersecurity measures, 4GuysCoffee can create a more secure environment for our business operations, customer data, and intellectual

property. Taking a proactive approach to cybersecurity helps protect against potential threats and enhances trust and confidence among customers and stakeholders.

Emerging threats and trends

Emerging threats in the cybersecurity landscape continue to evolve, presenting new challenges for organisations like 4GuysCoffee. One emerging threat is the proliferation of ransomware attacks, where cybercriminals encrypt sensitive data and demand ransom payments for release. These attacks have become increasingly sophisticated, targeting businesses of all sizes and industries, including those in the food and beverage sector. The financial and reputational damage caused by ransomware attacks can be significant, underscoring the importance of robust cybersecurity measures to mitigate this risk.

Another emerging threat is the rise of insider threats, where employees or contractors with access to sensitive information intentionally or unintentionally compromise data security. Insider threats can include malicious actions, such as data theft or sabotage, and unintentional mistakes resulting in data breaches. With the expanding reliance on remote work and cloud-based collaboration tools, the risk of insider threats has grown, highlighting the need for organisations to implement effective monitoring and access control measures to detect and prevent insider attacks.

Additionally, supply chain cyber attacks have emerged as a prominent threat, targeting vulnerabilities in the interconnected networks of suppliers, vendors, and partners. Cybercriminals exploit weaknesses in supply chain ecosystems to gain unauthorised access to valuable data or disrupt business operations. These attacks can have far-reaching consequences, affecting multiple organisations across various industries. As organisations like 4GuysCoffee rely on a global network of suppliers and partners, securing the supply chain against cyber threats has become a critical priority to safeguard business continuity and resilience.

Moreover, the increasing adoption of Internet of Things (IoT) devices introduces new vulnerabilities and attack vectors for cybercriminals to exploit. IoT devices, such as smart coffee machines or inventory management systems, often lack robust security features, making them susceptible to exploitation. Compromised IoT devices can be used as entry points into corporate networks, allowing cybercriminals to launch attacks or steal sensitive data. As 4GuysCoffee integrates IoT technologies into its operations, addressing the security risks associated with IoT devices is essential to prevent potential breaches and protect against emerging threats in the digital landscape.

In response to these emerging threats, we must remain vigilant and proactive in our approach to cybersecurity. This includes implementing advanced threat detection and response capabilities, enhancing employee cybersecurity awareness training, and strengthening partnerships with suppliers and vendors to ensure supply chain security.

Organisations like 4GuysCoffee can effectively mitigate risks and protect their assets against evolving cyber threats by staying informed about emerging threats and adopting a proactive cybersecurity posture.

Asset Inventory

Inventory of organisational assets

#	Asset	Model / S/N	Description	Value (S$ p.a.)
1	PC-1	Dell XPS Desktop (13th Gen Intel® Core™ i7-13700)	Main PC in HQ that hosts our web server (Apache HTTP Server 2.4.59 R2024-04-04)	$285.00 (running cost: considering the current electricity rate at 0.3247 GST inclusive, multiplied by the Desktop usage (kWh) of 100×24/1000 =2.4 kWh/day) Excludes: $2,500.00 (one-time unit cost)
2	PC-2	Dell XPS Desktop (13th Gen Intel® Core™ i7-13700)	Main PC in HQ that hosts our database (MariaDB 10.7.11)	$285.00 (running cost: considering the current electricity rate at 0.3247 GST inclusive, multiplied by the Desktop usage (kWh) of 100×24/1000 =2.4 kWh/day) Excludes: $2,500.00 (one-time unit cost)
3	Edge Router	Cisco RV160 VPN Router	Edge router - end point of private network, start point of public network	$2,000.00 (one-time cost)
4	Security Camera	Reolink RLC-410	18 cameras (3 for each of our 6 outlets + 8 for HQ)	$2,600.00 (maintenance outsourced to Lion Securisia Engineering LLP) Excludes: $2,860.00 (one-time cost)
5	Coffee Machine	Nuova Simonelli Appia II	6 units for all outlets	$2,600.00 (maintenance fee) Excludes: $24,000.00 (one-time cost)
6	POS	Shopify POS	Point of Sale System that processes transactions from our retail customers	$1,500.00 (monthly subscription)
7	Undercounter Refrigerator	True TUC-27	6 units for all outlets	$1,200.00 (maintenance fee) Excludes: $30,000.00 (one-time cost)
8	Commercial Refrigerator	Turbo Air M3R47-2	6 units for all outlets	$1,800.00 (maintenance fee) Excludes: $60,000.00 (one-time cost)

Classification of assets

1	Data	- **Employee Data**: Confidential information such as personal details, salary, and performance evaluations that require protection to maintain employee privacy and comply with regulatory requirements. - **Customer Data**: Critical information, including personal and financial details, that if compromised, could damage customer trust and reputation.
2	Hardware	- **Firewall, Server, PC, Web Server, Edge Router, POS:** Essential components of our network infrastructure that require protection to prevent unauthorised access and ensure system availability.
3	Intellectual Property	- **Customer Information**: Crucial for personalised services and marketing strategies, safeguarding customer information is essential to maintain loyalty and brand reputation. - **Physical and Digital Documents**: Protocols, recipes, and proprietary methods must be protected to prevent unauthorised use or replication by competitors.
4	People	- **C-level Executives**: Critical individuals whose access to sensitive information and decision-making authority makes them high-value cyberattack targets. - **Normal Employees**: While not as high-profile as C-level executives, normal employees play a crucial role in daily operations and must be protected to prevent unauthorised access to critical systems and data.
5	Procedures	- **Business Continuity Plan (BCP)**: A critical document outlining procedures for maintaining business operations during and after disruptive events. Its confidentiality is paramount to ensure the effectiveness of our response to crises. - **Standard Operating Procedures (SOP)**: Essential guidelines for employees to follow in various scenarios, contributing to operational efficiency and compliance. - **Supply Chain Management**: While not always confidential, sensitive information regarding suppliers, vendors, and partners must be protected to prevent disruptions and maintain competitive advantage.
6	Property	- **Cafe Outlets:** Critical assets that represent the face of our brand and must be protected from physical threats, vandalism, or theft. - **Physical Inventory:** Crucial for maintaining supply chain operations and fulfilling customer orders, safeguarding physical inventory is essential to prevent disruptions.
7	Software	- **Security Information and Event Management (SIEM)**: Critical for monitoring and detecting security incidents, ensuring the integrity and availability of our systems. - **Operating System (OS), Active Directory (AD), Database (DB)**: Core components of our IT infrastructure that require protection to prevent unauthorised access or data breaches.

Weighted Factor Analysis for Prioritisation

Information Asset	Criteria 1: Impact on Revenue	Criteria 2: Impact on Profitability	Criteria 3: Impact on Public Image	Weighted Score
Weight Score	*30*	*40*	*30*	*100*
Trade Secret	0.4	0.4	0.6	**46**
Customer Information	0.6	0.5	0.9	**65**
Employee Information	0.6	0.5	0.7	**59**
Database	0.8	0.9	0.6	**78**
Edge Router	0.9	0.9	0.7	**84**
Firewall	0.9	0.9	0.9	**90**
Web Server	0.7	0.8	0.8	**77**
Cafe Equipment (PoS, coffee machines etc)	0.8	0.8	0.6	**74**

Justification

Firewall has the highest weighted score of 90, indicating it has the most significant combined impact on revenue, profitability, and public image. This is due to firewalls' critical role in protecting our network and data, directly affecting the company's profitability and public image.

Edge Router follows with a score of 84. Edge routers are crucial for network security and connectivity. While they may not directly impact revenue or profitability, any disruption or compromise could lead to negative public perception, mainly if it affects service availability or data security.

Database and Cafe Equipment have similar impacts, with scores of 78 and 74, respectively. Databases are central to our operations and can impact revenue and profitability if compromised. Databases often contain sensitive information, including customer and employee data. A compromise of the database could significantly impact revenue, profitability, and public image, warranting high scores across all criteria. Cafe Equipment, like point-of-sale systems and coffee machines, can directly impact revenue and profitability in a cafe setting. POS systems directly handle revenue-generating transactions, making them vital for revenue and profitability. Additionally, a breach of POS systems could damage public trust in the organisation's ability to protect customer payment information.

Customer Information and Web Server both scored 65 and 77, respectively. Handling customer information can significantly impact a company's public image and profitability. Customer information is crucial for revenue generation and maintaining profitability. A customer data breach could result in financial losses due to legal fines, lawsuits, and company reputation damage. Therefore, it scores high in the Impact on Revenue and Profitability criteria.
On the other hand, web servers are crucial for maintaining an online presence and doing business online. While it may not directly impact revenue or profitability, any disruption or compromise could lead to negative public perception, mainly if it affects service availability or data security.

Employee Information and Trade Secret are at the lower end with scores of 47 and 65, respectively. Employee information is essential for operational purposes, but its impact on revenue and profitability may be lower than that of customer information. However, a breach of employee data could still negatively impact the public image, primarily if it affects employee trust and morale. While important, they may not have as immediate or direct an impact on revenue or profitability as the other assets. While it may not directly impact revenue or profitability, a compromise of trade secrets could significantly negatively affect the organisation's public image, potentially leading to a loss of trust from customers and stakeholders. Therefore, it receives a relatively higher score in the Impact on Public Image criterion.

Identifying possible vulnerabilities for the prioritised assets

Assets	**Vulnerabilities**	**Threats**
Firewall	• Weak Access Controls • Unpatched Bugs	• DoS Attacks - attackers may overwhelm the firewall • Unauthorised access - gain access over the firewall to gain access to the internal network
Database	• Unnecessary permissions • Unencrypted data	• SQL Injection Attacks • Insider threats • Data breaches
Operating System	• Outdated software • Weak password strength	• Insider Threats • Malware
Web Server	• Weak web application security • Outdated software	• Web defacement • Malware distribution • Lateral/Vertical Penetration
Edge Router	• Misconfigurations • Outdated Firmware • Unencrypted traffic • Single Point of Failure	• MiTM attacks • Routing Protocol Attacks

TVA Worksheet

Threat No.	Explanation
T1	Denial of Service (DoS)
T2	Insider Threats
T3	SQL Injection
T4	Malware
T5	Social Engineering
T6	Physical Theft/Damage
T7	Data Breach
T8	Man In The Middle Attack
T9	Web Defacement
T10	Ransomware

Asset Code	Asset Type	Asset Name	Description
A1	Data	Customer Information	Customer's full name, NRIC, address, email.
A2	Data	Employee Records	It is similar to customer information but has designation and salary information included.
A3	Intellectual Property	Trade Secret	Recipes, business strategy and plan.
A4	Hardware	Edge Router	Router responsible for connecting LAN to the internet.
A5	Hardware	Firewall	Module used for network security such as Palo Alto.
A6	Hardware	Web Server	Computer used to serve web data to browsers connected to the internet.
A7	Software	Operating Systems	Software installed that provides an interface for users to manage resources such as files and directories etc.
A8	Hardware	Database Server	A computer dedicated to running the database which stores customers' information including card details etc.
A9	Hardware	Cafe Equipment	Espresso machine, grinder, POS etc.
A10	Hardware	Workstations	Physical devices assigned to employees such as laptops, tablets, and work phones.

The top 5 most valuable assets are listed below in order, along with their probable vulnerabilities.

Ref.	Assets	Vulnerability Description
T7V1A8	A8: Database Server	Misconfiguration of software, which actors can exploit to disclose customers' sensitive information for purposes such as tarnishing the company's image as a competitor and/or financial reward such as selling the information on the dark web.
T4V2A8		A specialised type of malware - financial malware may be used to scan computers or a network to retrieve transaction information.
T10V1A7	A7: Operating Systems	Software with known (usually outdated software) or unknown (zero-day attacks) can be prone to unauthorised access where manipulation of resources such as the deletion or encryption of crucial files - ransomware.
T4V2A7		Generic malware may infect the system and the OS by downloading suspicious attachments, browsing unsecured websites etc., which may detrimentally affect the computer's performance.
T8V1A5	A5: Firewall	Misconfiguration of the firewall could lead to unauthorised access by a malicious threat actor that enables the actor to monitor network traffic between the intranet and the internet.
T2V2A5		Unsatisfied employees or carelessness can lead to implementing policies on the firewall that enable incoming traffic from a particular IP address or a range of IP addresses, thus maintaining access to the firewall.
T1V1A4	A4: Edge Router	Edge routers are often a single point of contact between the intranet and internet as it facilitates ease of monitoring and configuration. Hence, this deems them as a popular target for DoS attacks and thus leaving the company unable to access the internet.
T2V2A4		Malicious insiders may gain access to the internet-facing router through vulnerabilities such as outdated OS, poor password hygiene and set static routes to route traffic to a malicious host.
T6V1A6	A6: Web Server	Unused open ports may be exploited for the attacker to gain access to the web server where they may modify the web files to change the appearance and information displayed on the website.
T3V2A6		Poor code sanitisation may lead to attackers being able to execute SQL injection commands to view confidential information.

A1-A5

	Assets Referral	A1	A2	A3	A4	A5
Threats Referral	Threats/Assets	Cust. Info (4)	Employee Records (4)	Database Server (5)	Edge Router (5)	Firewall (6)
T1	DoS (5)	x	x	x	T1V1A4	T1V3A5
T2	Insider Threats (10)	T2V3A1	T2V3A2	T2V3A3	T2V2A4	T2V2A5
T3	SQL Injection (2)	x	x	T3V5A3	x	x
T4	Malware (4)	x	x	T4V2A3	x	x
T5	Social Engineering (10)	T5V1A1	T5V1A2	T5V1A3	T5V3A4	T5V4A5
T6	Physical Theft (3)	x	x	x	T6V5A4	T6V6A5
T7	Data Breach/Leak (7)	T7V4A1	T7V4A2	T7V4A3	x	T7V5A5
T8	MiTM (3)	x	x	x	T5V4A4	T8V1A5
T9	Web Defacement (1)	x	x	x	x	x
T10	Ransomware (4)	T10V3A1	T10V2A10	x	x	x

A6-A10

	Assets Referral	A6	A7	A8	A9	A10
Threats Referral	Threats/Assets	Web Server (8)	OS (6)	Trade Secret (3)	Cafe Eq. (3)	Workstations (5)
T1	DoS	T1V3A6	T1V3A7	x	x	T1V1A10
T2	Insider Threats	T2V4A6	T2V4A7	T2V1A8	T2V2A9	T2V2A10
T3	SQL Injection	T3V2A6	x	x	x	x
T4	Malware	T4V5A6	T4V2A7	x	x	T4V3A10
T5	Social Engineering	T5V6A6	T5V5A7	T5V2A8	T5V3A9	T5V4A10
T6	Physical Theft	x	x	x	T6V4A9	x
T7	Data Breach/Leak	T7V1A6	T7V6A7	T7V3A8	x	x
T8	MiTM	x	x	x	x	T8V7A10
T9	Web Defacement	T6V7A6	x	x	x	x
T10	Ransomware	T10V8A6	T10V1A7	x	x	x

	A6	A5	A7	A3	A4	A10	A1	A2	A8	A9
T2	T2V4A6	T2V2A5	T2V4A7	T2V3A3	T2V2A4	T2V2A10	T2V3A1	T2V3A2	T2V1A8	T2V2A9
T5	T5V6A6	T5V4A5	T5V5A7	T5V1A3	T5V3A4	T5V4A10	T5V1A1	T5V1A2	T5V2A8	T5V3A9
T7	T7V1A6	T7V5A5	T7V6A7	T7V4A3	X	X	T7V4A1	T7V4A3	T7V3A8	X
T1	T1V3A6	T1V3A5	T1V3A7	X	T1V1A4	T1V1A10	X	X	X	X
T4	T4V5A6	X	T4V2A7	T4V2A3	X	T4V3A10	X	X	X	
T10	T10V8A6	X	T10V1A7	X	X	X	T10V3A1	T10V2A10	X	X
T6	X	T6V6A5	X	X	T6V5A4	X	X	X	X	T6V4A9
T8	X	T8V1A5	X	X	T5V4A4	T8V7A10	X	X	X	X
T3	T3V2A6	X	X	T3V5A3	X	X	X	X	X	X
T9	T6V7A6	X	X	X	X	X	X	X	X	X
Priority of Control	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

Impact Analysis

Determining the impact following successful threat exploitation of a vulnerability belonging to an asset. The system and information owners are responsible for determining this impact level for their own system and information. Usually, the appropriate way is to interview and obtain this information from the system and information owners themselves. It is categorised into three qualitative categories: low, medium, and high. The impact of a security event can also be rated against the CIA triad.

	Confidentiality	Integrity	Availability
Low	Loss of confidentiality leads to a **limited effect** on the organization.	Loss of integrity leads to a **limited effect** on the organization.	Loss of availability leads to a **limited effect** on the organization.
Moderate	Loss of confidentiality leads to a **serious effect** on the organization.	Loss of integrity leads to a **serious effect** on the organization.	Loss of availability leads to a **serious effect** on the organization.
High	Loss of confidentiality leads to a **severe effect** on the organization.	Loss of integrity leads to a **severe effect** on the organization.	Loss of availability leads to a **severe effect** on the organization.

Asset	Confidentiality	Integrity	Availability
Firewall	Moderate	High	High
Edge Router	Moderate	High	High
Web Server	High	High	High
Operating systems	Moderate	High	High
Database server	High	High	High

A compromised firewall could allow unauthorised access to confidential data. It's crucial for maintaining data privacy. A firewall with vulnerabilities could allow manipulation of data packets, affecting integrity. A malfunctioning firewall could block legitimate traffic, impacting the availability of resources.

Similar to a firewall, a compromised router could expose sensitive information. Routing manipulation could send data to unintended destinations, affecting integrity. A router outage could disrupt network connectivity, impacting the availability of resources.

Web servers often store sensitive user data like login credentials. A compromised server could lead to data breaches. Tampering with web server files could lead to displaying incorrect or malicious content, impacting data integrity. A web server crash would prevent users from accessing the website, impacting availability.

Database servers store the heart of an organisation's data. A breach could expose critical information. Database corruption could render data unusable, impacting integrity. A database server outage would prevent applications from accessing data, impacting availability.

Many operating system vulnerabilities can expose sensitive information stored locally. Unpatched vulnerabilities could allow attackers to tamper with system files, impacting

integrity. OS crashes or malware infections could render systems unusable, impacting availability.

Ranked Vulnerability Risk Worksheet

Asset	Asset Impact (AI)	Vulnerability	Vulnerability Likelihood (VL)	Risk Rating Factor (AI x VL)
Edge Router	84	Internet disruption due to DoS attack	0.8	67.2
Firewall	90	Unauthorised access as root user due to OS command injection (recent exploit in 2024 for Palo Alto)	0.9	81
Web Server	77	Unauthorised login or loss of confidential data due to SQL Injection	0.9	69.3
Operating Systems	80	System crashes due to file injections	0.6	48
Database Server	78	Loss of confidential data due to misconfiguration like weak credentials	0.95	74.1

Edge router: Attackers can exploit vulnerabilities to overwhelm the router with traffic, rendering it unavailable to legitimate users. This is a common tactic to disrupt operations or distract defenders. These vulnerabilities are well-known and actively exploited by attackers. Keeping firmware up-to-date and using strong credentials helps mitigate these risks.

Firewall: This recently discovered vulnerability in PAN-OS versions 10.2, 11.0, and 11.1 with specific configurations could allow unauthenticated attackers to execute arbitrary code with root privileges, potentially giving them complete control over the firewall. Patches have been released, so updating is critical: https://unit42.paloaltonetworks.com/cve-2024-3400/. The recent OS command injection vulnerability (CVE-2024-3400) is a serious concern due to its potential impact and exploitability.

Web server: SQLi and XSS are widespread vulnerabilities with readily available exploit tools. Constant vigilance and secure coding practices are crucial.
Operating systems: Vulnerabilities that allow attackers to inject malicious code into files can lead to unauthorised access or system compromise. File injection vulnerabilities are less common but still pose a threat.

Database servers: Improper database configuration, like weak credentials or unnecessary privileges, can open the database for exploitation. Misconfiguration is also common due to human error or a lack of awareness.

Cost-Benefit Analysis:

Overview

This section will delve into the critical assets pivotal to 4GuysCoffee's operations, primarily focusing on costings. These assets represent the foundation of our business activities, and any disruption to their functionality could significantly impede our ability to serve customers and manage day-to-day operations. By conducting a cost-benefit analysis of these critical assets, we aim to gain insights into the financial implications of potential security threats and the effectiveness of our current risk mitigation strategies. This approach will enable us to make informed decisions regarding resource allocation and prioritise investments in security measures that provide the greatest value and protection for our organisation.

Assets and Valuation Table:

Asset	Value
Web Server	$2500.00
Database	$3500.00
Account Management (AD)	$2000.00
Edge Router	$1000.00
Wireless Access Point (WAP)	$800.00
Point of Sale	$3000.00
Social Media Account	$10000.00
Total	**$22800**

Justification for asset valuation:

Web Server:

- **Justification**: The web server hosts our cafe's website and online ordering system. It is the primary interface for customers to view our menu, place orders, and learn about our business. Therefore, its availability, performance, and security directly impact revenue generation and customer satisfaction.

2. **Database**:
    - **Justification**: The database holds critical data such as staff information, customer records, transaction history, and inventory details. This data is essential for day-to-day operations, including managing staff schedules, processing orders, tracking inventory levels, and analysing customer preferences. The integrity, security, and accessibility of this data are paramount for maintaining operational efficiency and providing quality service.

3. **Account Management (AD)**:
    - **Justification**: The Account Management system (Active Directory or AD) controls access to sensitive data and network resources within our organisation. It manages user accounts, permissions, and authentication processes, ensuring secure access to company systems and resources. Any compromise to the AD system could result in unauthorised access to sensitive information, network breaches, or disruptions to business operations, making it a critical asset for security and operational integrity.

4. **Edge Router**:
    - **Justification**: The edge router is the gateway between our internal network and the internet. It manages incoming and outgoing network traffic, enforces security policies, and connects our cafe's various devices and systems. The router's stability, performance, and security features are crucial for maintaining reliable internet connectivity, protecting against cyber threats, and ensuring uninterrupted business operations.

5. **Wireless Access Point (WAP)**:
    - **Justification**: The Wireless Access Point (WAP) provides wireless network connectivity to our cafe's customers and staff. It enables seamless internet access for customers, supports mobile payment systems, and facilitates the use of digital devices for ordering, browsing, and entertainment. Reliable Wi-Fi connectivity enhances the customer experience, encourages longer stays, and promotes customer engagement with our cafe's digital services.

6. **Point of Sale (Shopify)**:
    - **Justification**: The Point of Sale (POS) system, powered by Shopify, is the central hub for processing transactions, managing inventory, and analysing sales data. It streamlines the checkout process, tracks inventory levels in real time, and provides valuable insights into customer purchasing behaviour and trends. The POS system's reliability, functionality, and integration capabilities are essential for optimising sales operations, maximising revenue, and delivering a seamless shopping experience for customers.

7. **Social Media Account**:
    - **Justification**: Our social media account is a crucial platform for marketing, brand promotion, customer engagement, and community building. It allows us to reach and interact with a wide audience, showcase our cafe's offerings, share updates and promotions, and engage with customers in real time. The account's follower base represents a valuable audience interested in our cafe's products and services, offering opportunities for direct communication, feedback collection, and brand advocacy.

      Additionally, our social media presence contributes to brand visibility, customer acquisition, and retention, influencing purchasing decisions and driving traffic to your physical location and online channels.
      Therefore, the social media account is a key marketing and communication asset, contributing to brand awareness, customer engagement, and revenue growth. Its valuation encompasses follower demographics, engagement rates, conversion potential, and its role in overall brand strategy and market positioning.

By considering these factors, we justify the adjusted valuations of each asset, taking into account their critical role in supporting our cafe's operations, ensuring data security, and driving revenue generation.

Cost-Benefit Analysis Table (Pre-Control)

AV = Asset Value | EF = Exposure Factor
SLE = Single Loss Expectancy (AV x EF) | ARO = Annualised Rate of Occurrence
ALE = Annual Loss Expectancy (SLE x ARO) | ACS = Annualised Cost of Safeguards
CBA = Cost-Benefit Analysis (ALEpre - ALEpost - ACS)

Asset	Risk	AV	EF	SLE	ARO	ALE
Web Server	Malware Injection	$2500	0.8 (H)	$2000	1	$2000
Database	Data Breach	$3500	0.6 (M)	$2100	0.5	$1050
Account Management (AD)	Malware Injection	$2000	0.8 (H)	$1600	1	$1600
Edge Router	Malware Injection (Firmware Vuln.)	$1000	0.8 (H)	$800	1	$800
Wireless Access Point (WAP)	Malware Injection	$800	0.8 (H)	$640	1	$640
Point of Sale	Malware Injection	$3000	0.8 (H)	$2400	1	$2400
Social Media Account	Account Hacking	$10000	0.7 (H)	$7000	0.5	$3500
Total		**$22800**		**$16540**		**$11990**

Combined Cost of Security Controls

Control	Cost (S$ p.a.)
Wazuh SIEM (t2.small)	$201.48
Palo Alto Firewall	$250
Learning Management System	$1788
Total	**$2329.48**

Pooling the expenses for Security Information and Event Management (SIEM), Firewall, and Learning Management System (LMS) and allocating them to individual assets is a logical approach for 4GuysCoffee. It ensures that our security budget is efficiently managed while guaranteeing comprehensive protection for our infrastructure. Given that the costs for SIEM, Firewall, and LMS are typically incurred annually and benefit the entire network environment, dividing these expenses among assets provides a fair and accurate distribution of resources. This strategy promotes cost-effectiveness and allows for a more tailored allocation of security spending based on the risk profile and importance of each asset within our organisation. Ultimately, consolidating these costs simplifies financial management and optimises the effectiveness of our security investments across all assets, reinforcing our commitment to safeguarding 4GuysCoffee's digital infrastructure.

Extended Cost-Benefit Analysis Table (Post Control)

Asset	Risk	AV	EF	SLE	ARO_{post}	ALE_{pre}	ALE_{post}	ACS	CBA
Web Server	Malware Injection	$2500	0.8 (H)	$2000	0.2	$2000	$400	SIEM/FW/LMS ($320)	$1280
Database	Data Breach	$3500	0.6 (M)	$2100	0.3	$1050	$630	SIEM/FW/LMS ($320)	$100
Account Management (AD)	Malware Injection	$2000	0.8 (H)	$1600	0.2	$1600	$320	SIEM/FW/LMS ($320)	$960
Edge Router	Malware Injection (Firmware Vuln.)	$1000	0.8 (H)	$800	0.2	$800	$160	SIEM/FW/LMS ($320)	$320
Wireless Access Point (WAP)	Malware Injection	$800	0.8 (H)	$640	0.2	$640	$128	SIEM/FW/LMS ($320)	$192

Point of Sale	Malware Injection	$3000	0.8 (H)	$2400	0.2	$2400	$480	SIEM/FW/LMS ($320)	$1600
Social Media Account	Account Hacking	$10000	0.7 (H)	$7000	0.25	$3500	$875	SIEM/FW/LMS ($320)	$2305
Total		**$22800**		**$16540**		**$11990**	**$2993**		**$6757**

Justification

1. **Malware Injection:** Malware injection presents a significant threat to our organisation, with a high likelihood of occurrence. Malware, malicious software designed to disrupt, damage, or gain unauthorised access to computer systems, can infiltrate our network through various vectors such as phishing emails, malicious websites, or compromised software. Once injected, malware can wreak havoc by stealing sensitive data, compromising system integrity, or facilitating further cyber attacks. According to the Verizon Data Breach Investigations Report 2021, malware attacks remain one of the most common and damaging threats organisations worldwide face, underscoring the critical importance of robust cybersecurity measures to defend against this pervasive threat.

2. **Data Breach**: While data breaches can have serious consequences, they may not always result in immediate financial or reputational damage. The severity of data breaches can vary depending on the sensitivity and volume of the compromised data.

3. **Account Hacking:** Account hacking incidents can severely damage the organisation's reputation and erode customer, partner, and stakeholder trust. Hackers could exploit authentication system vulnerabilities or use techniques like phishing to gain unauthorised access to our social media accounts. Publicised breaches can lead to negative media coverage, loss of customer confidence, and long-term damage to the brand's image, resulting in market share and competitive disadvantage.

Post-Control Effect

The data provided offers valuable insights into the risk management and security posture of 4GuysCoffee, highlighting the effectiveness of implemented controls and their impact on mitigating identified risks.

Firstly, the identified risks assets face—Malware Injections, Data Breaches, and Account Hacking—are common threats in today's digital landscape, particularly for organisations handling sensitive data such as customer information and financial transactions. These risks pose significant financial and reputational consequences if left unaddressed.

The controls implemented—Wazuh SIEM, Palo Alto Firewall, and Learning Management System (LMS)—are crucial in mitigating these risks. Past incidents have demonstrated the effectiveness of these controls in successfully detecting and remediating security threats. For instance, the Wazuh SIEM provides real-time monitoring and analysis of security events, enabling prompt detection and response to malware injections and unauthorised access attempts. The Palo Alto Firewall offers robust network protection, preventing data breaches by filtering malicious traffic and enforcing security policies. Additionally, the Learning Management System (LMS) enhances employee awareness and compliance with security protocols, reducing the risk of account hacking through phishing attacks or weak password practices.

The analysis also considers the financial implications of implementing these controls. With an ALE (Annual Loss Expectancy) pre-control of $11,990 reduced to $2,993 post-control, the controls have significantly reduced the potential financial losses associated with security incidents. The combined cost of security controls, at $320 per asset, demonstrates a cost-effective investment in mitigating risks and protecting the organisation's assets and reputation.

Furthermore, it is important to note that while the implemented controls may be considered entry-level, their effectiveness in addressing the specific security needs of an SME like 4GuysCoffee should not be underestimated. Despite being an entry-level subscription, the Palo Alto Firewall provides sufficient network security features to defend against common cyber threats small to medium-sized businesses face.

In a nutshell, the data analysis underscores the importance of proactive risk management and the value of investing in appropriate security controls tailored to the needs and resources of the organisation. By effectively addressing identified risks and minimising potential losses, 4GuysCoffee can maintain a strong security posture and safeguard its operations in an increasingly digital world.

Controls and Countermeasures

Description of security controls in place

At 4GuysCoffee, safeguarding our digital assets is a cornerstone of our operational ethos. In light of a recent cyberattack, we've taken decisive action to fortify our defences, recognising the ever-present threat landscape. Our response has been twofold: first, the adoption of a cutting-edge Security Information and Event Management (SIEM) tool, and second, a strategic move towards cloud-based security solutions. Additionally, it's worth noting that before this incident, we already had existing security measures, particularly within our Active Directory and Network Infrastructure. These measures include but are not limited to Group Policy Objects to enforce security measures like strict password policies, as well as Access Control Lists, which have contributed to our overall security posture.

As highlighted earlier, we have opted to host the esteemed open-source SIEM solution, Wazuh, to leverage cloud technology on our AWS EC2 platform. This strategic decision

affords us unparalleled scalability and flexibility, which are crucial in the ever-changing cybersecurity landscape. We balance security efficacy and operational efficiency by harnessing AWS's suite of managed services and selecting cost-effective instance types. This pragmatic approach not only enhances our ability to detect and respond to threats promptly but also optimises resource utilisation, ensuring we maximise value without compromising on security.

Our unwavering commitment to cybersecurity extends beyond mere technological solutions—it's about safeguarding the trust and confidence of our stakeholders. Through ongoing innovation, vigilance, and collaboration, we're dedicated to maintaining the integrity of our critical assets and upholding the highest standards of security excellence.

Categories of security controls

		Control Types		
		Physical	**Technical**	**Administrative**
Control Functions	**Preventive**	Biometric Scanners	Firewall	Security policies & procedures
		Access Cards	Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)	Security awareness training
		Security Guards	Encryption	Access management
		Surveillance Systems	Antivirus/Anti-malware software	Incident response plan
		Environmental Controls		
	Detective	CCTV Cameras	Logging and monitoring systems	Regular security audits and vulnerability assessments
		Motion sensors	Security Information and Event Management (SIEM)	Anomaly detection mechanisms
				Security incident response procedures and Playbooks
	Corrective	Fire suppression systems	Regular patching and updating	Backup and disaster recovery solutions
		Temperature controls	Conducting post-incident reviews	Updating security controls
		Humidity sensors	Conducting root cause analysis	

Evaluation of control effectiveness

Given recent cybersecurity challenges, 4GuysCoffee thoroughly evaluated our security controls to fortify our defences against evolving threats. This scrutiny revealed a pressing need for a multifaceted approach, blending advanced technologies and cloud-based solutions to bolster our resilience.

Leveraging Advanced Technologies:

Adopting a Security Information and Event Management (SIEM) tool became a pivotal strategy in our defence arsenal. This SIEM solution tirelessly monitors our digital boundaries in real time. Its prowess extends beyond mere surveillance, enabling comprehensive vulnerability assessments to identify and rectify security weaknesses proactively. Hosting the open-source SIEM platform, Wazuh, on our AWS EC2 infrastructure provides scalability and flexibility vital in navigating the dynamic cybersecurity landscape. By harnessing AWS's suite of managed services and cost-effective instance types, we balance security efficacy and operational efficiency, ensuring optimal resource utilisation without compromising protection.

Diverse Security Controls:

Our security controls encompass a spectrum of physical, technical, and administrative measures, each playing a distinct role in fortifying our defences. Biometric scanners and access cards act as sentinels, preventing unauthorised access, while CCTV cameras and logging systems serve as vigilant watchers, detecting anomalous activities. Fire suppression systems and routine patching are corrective measures to mitigate risks and respond effectively to incidents. Regular security audits, vulnerability assessments, and post-incident reviews provide valuable insights into control effectiveness and areas for improvement.

Recommendations for improvement

Strengthening Security Awareness:

Investing in comprehensive security awareness training programs is paramount to fostering a culture of vigilance among our workforce. Enhancing employees' understanding of emerging cybersecurity threats and best practices empowers them to become proactive guardians of our digital assets. These training programs should cover phishing awareness, password hygiene, social engineering tactics, and reporting suspicious activities. Interactive workshops, simulated phishing exercises, and regular security updates can keep employees engaged and informed. Additionally, creating a reporting mechanism for security concerns and incidents encourages a collaborative approach to threat detection and response, fostering a culture of collective responsibility for cybersecurity.

Enhanced Anomaly Detection:

Deploying advanced anomaly detection mechanisms can bolster our ability to promptly detect and respond to emerging threats. In addition to traditional security controls, we can leverage cutting-edge technologies such as machine learning and behavioural analytics. These solutions can analyse vast amounts of data to identify deviations from standard patterns of

behaviour, flagging potential security incidents in real time. We can proactively identify and mitigate suspicious activities by continuously monitoring network traffic, user activities, and system logs before they escalate into full-blown security breaches. Regularly updating and fine-tuning these anomaly detection systems ensures their effectiveness in detecting evolving threats.

Robust Incident Response Procedures:
Developing and refining robust incident response procedures is critical to minimising the impact of security incidents. By establishing clear protocols and playbooks, we can streamline our response efforts and effectively mitigate the consequences of breaches. Incident response plans should outline the roles and responsibilities of key stakeholders, the escalation process, communication protocols, and steps for containment, eradication, and recovery. Regular tabletop exercises and simulations helps validate the effectiveness of these procedures and familiarises the response team with their roles in a controlled environment. Additionally, establishing partnerships with external incident response teams and legal experts ensures access to additional resources and expertise during crises.

Regular Updates and Patching:
Prioritising regular updates and patching of security controls is essential to remediate known vulnerabilities and strengthen our defences against emerging threats. Proactively applying patches and updates to operating systems, software applications, and security tools closes known security gaps and reduces the risk of exploitation by malicious actors. Implementing an automated patch management system can streamline the update process and ensure the timely deployment of patches across the organisation's infrastructure. Regular vulnerability scanning and penetration testing further validate the effectiveness of patching efforts and identify any remaining security weaknesses that require attention.

Resilient Backup and Recovery Solutions:
Implementing robust backup and disaster recovery solutions is essential to ensure business continuity during a security incident. By regularly backing up critical data and testing recovery procedures, we can minimise downtime and mitigate the impact of disruptions. Utilising cloud-based backup solutions provides scalability and redundancy, ensuring that data remains accessible even in the event of localised outages or hardware failures. Developing a comprehensive data retention policy helps prioritise backup efforts and determine the frequency and granularity of backups based on the criticality of the data. Regularly testing backup integrity and recovery procedures ensures their effectiveness and helps identify gaps or issues we must address. Additionally, establishing off-site backup locations and leveraging encryption techniques protect backup data from unauthorised access or tampering, further enhancing resilience against potential threats.

Training and Awareness

Overview of security awareness programs

At 4GuysCoffee, we understand that human error can be a significant vulnerability in cybersecurity, making it crucial to prioritise awareness and education among our workforce.

To address this, we've developed comprehensive security awareness programs to empower our employees to effectively recognise and mitigate potential security risks.

Our primary objective is to instil a culture of security consciousness throughout our organisation, from frontline staff to senior executives. By fostering a proactive mindset towards security, we aim to reduce the likelihood of security incidents occurring and minimise the impact of any breaches that may occur. Through regular training sessions, workshops, and communication initiatives, we strive to ensure that every team member understands the importance of their role in safeguarding sensitive information.

Our programs are designed to equip employees with the knowledge and skills necessary to protect our data assets' integrity, confidentiality, and availability. By enhancing awareness of common threats such as phishing scams, social engineering attacks, and password security best practices, we empower our workforce to identify and respond to potential risks effectively.

Ultimately, our goal is to create a security-aware culture where every employee feels personally invested in maintaining the security of our information assets. Through ongoing education and engagement, we aim to build a resilient defence against cyber threats and uphold our customers' and stakeholders' trust and confidence.

Components of the security awareness programs

The security awareness programs at 4GuysCoffee consist of several key components to educate and empower our employees to mitigate cybersecurity risks effectively.

- Regular Training Sessions: These sessions are held quarterly and cover essential security topics such as identifying phishing attempts, maintaining strong password hygiene, adhering to data handling procedures, and understanding compliance requirements. Tailored sessions are conducted for different departments to address specific security concerns relevant to their roles, ensuring all employees receive targeted training. Our quarterly training sessions are not just lectures but interactive forums where employees actively engage with cybersecurity concepts. For example, in a recent session, employees were presented with scenarios depicting social engineering attacks, such as a phone call from a purported IT technician requesting sensitive information. Through group discussions and guided analysis, employees learned to identify the signs of social engineering and the appropriate response protocols. By incorporating real-life examples and encouraging participation, these sessions foster a deeper understanding of cybersecurity principles and promote a proactive approach to security.

- Interactive Workshops and Simulations: Bi-annual workshops simulate real-world security scenarios, including mock phishing campaigns, incident response simulations, and role-playing scenarios. These interactive sessions enhance employee

preparedness and response capabilities during security incidents, providing hands-on experience in identifying and mitigating threats. In a recent workshop, employees participated in a tabletop exercise simulating a ransomware attack on our company's network. Through role-playing and scenario-based discussions, employees collaborated to develop and execute an incident response plan, including containment, eradication, and recovery procedures. These simulations strengthen employees' technical skills and cultivate teamwork and resilience in the face of cyber threats.

- Online Learning Resources: Our intranet portal hosts accessible e-learning modules covering various security topics. Employees can access self-paced courses, videos, and knowledge articles to deepen their understanding of cybersecurity fundamentals. Modules include recognising social engineering tactics, understanding regulatory compliance, and staying updated on emerging threats. For example, our module on "Data Privacy Essentials" provides practical tips for protecting sensitive information, such as encrypting emails and securing physical documents. Employees can also explore case studies and real-world examples to gain insights into common security pitfalls and best practices.

- Role-Based Training Tracks: Customised training tracks are tailored to different job roles and responsibilities within the organisation. IT staff receive specialised technical training on network security, system administration, and threat detection, while customer service representatives learn to handle customer data securely and respond to security-related inquiries. Cafe staff receive training on physical security measures, incident reporting procedures, and customer data protection. By aligning training content with job roles, we ensure each employee gets targeted instruction relevant to their daily tasks.

- Continuous Monitoring and Evaluation: Regular assessments and quizzes measure employee knowledge and awareness levels, allowing us to track progress and identify areas for improvement. For example, after completing a training module on phishing awareness, employees may participate in a simulated phishing exercise to test their newfound skills in a real-world context. Feedback mechanisms, such as surveys and focus groups, provide valuable insights into the effectiveness of training initiatives and inform future program enhancements. By fostering a culture of feedback and adaptation, we ensure that our security awareness program remains dynamic and responsive to emerging threats.

Policies and Procedures

Governance policies and procedures

Our Information Security GRC is underpinned by a comprehensive set of policies and procedures designed to guide the organisation's approach to information security. These policies are the foundation for ensuring our data assets' confidentiality, integrity, and availability.

Enterprise Information Security Policy (EISP): An Enterprise Information Security Policy (EISP) is a comprehensive document outlining an organisation protecting its information assets. It is a guiding framework for establishing, implementing, and maintaining effective information security practices across the organisation.

1. Statement of Purpose:

The Enterprise Information Security Policy (EISP) is the cornerstone of 4GuysCoffee's commitment to protecting its information assets. It outlines the organisation's dedication to maintaining data confidentiality, integrity, and availability, emphasising the importance of information security as a fundamental aspect of business operations. By clearly defining the policy's purpose, 4GuysCoffee aims to establish a unified direction and set expectations for all employees, contractors, and stakeholders regarding their roles and responsibilities in safeguarding sensitive information that employees abide by.

2. Information Security Elements:

At 4GuysCoffee, information security encompasses a comprehensive set of practices and principles to mitigate risks and protect valuable data assets. This includes access controls, encryption, intrusion detection, and security awareness training. The organisation's security philosophy prioritises proactive risk management, continuous monitoring, and adherence to industry best practices. By defining information security in this manner, 4GuysCoffee emphasises its commitment to maintaining the highest data protection standards and ensuring its customers' and stakeholders' trust and confidence.

3. Need for Information Security:

The need for robust information security measures cannot be overstated in today's digital age. As a retailer with an extensive online presence and a wealth of customer data, 4GuysCoffee faces constant threats from cyberattacks, data breaches, and other security incidents. Protecting sensitive information is an essential legal and ethical obligation to preserve customer trust and brand reputation. By prioritising information security, 4GuysCoffee demonstrates its dedication to responsible data stewardship and its commitment to safeguarding the interests of all stakeholders.

4. Roles and Responsibilities:

General Manager (GM): As the highest-ranking executive, the GM oversees governance, risk management, and compliance efforts. They ensure robust policies and procedures are established and effectively communicated throughout the organisation, promoting a security awareness and accountability culture.

Department Heads:

- Technology: Collaborates with the GM to develop and implement technology-related GRC policies and procedures, ensuring compliance with regulatory requirements and industry standards.

- Human Resources: Establishes and maintains HR policies that comply with employment laws and regulations, managing employee rights and data privacy risks.
- Customer Service: Implements policies to ensure compliance with customer service regulations, safeguarding customer data and maintaining high satisfaction and loyalty.
- Sales and Marketing: Develops and enforces policies related to marketing and sales practices, ensuring compliance with legal and regulatory requirements while maximising the effectiveness of marketing initiatives.
- Logistics: Develop policies for supply chain management and logistics operations, mitigating risks related to supply chain disruptions and ensuring business continuity.
- Roasting Facility and Cafe Operations: Establishes GRC policies for roasting facility and cafe operations, ensuring compliance with food safety regulations and maintaining product quality and integrity.

5. Reference to Other Standards and Guidelines:

The EISP at 4GuysCoffee aligns with internationally recognised standards and guidelines, including PDPA, GDPR, ISO/IEC 27001, NIST Cybersecurity Framework, and PCI DSS. These standards serve as benchmarks for evaluating the effectiveness of the organisation's security controls and help ensure compliance with legal and regulatory requirements. By referencing these standards, 4GuysCoffee demonstrates its commitment to maintaining a proactive and robust approach to information security that meets industry best practices and standards.

Issue-Specific Security Policy (ISSP):

The Issued Specific Security Policy (ISSP) is a targeted document that outlines specific guidelines and procedures for securing a particular aspect of an organisation's information systems. In this case, we developed an ISSP for Point-of-Sale (POS) systems, which are critical components of our business operations at 4GuysCoffee.

POS systems handle sensitive customer information, including payment card data, making them prime cyberattack targets. Therefore, it is essential to have a comprehensive security policy in place to safeguard these systems and the data they process. The ISSP for POS systems provides clear instructions for authorised users on securely using, managing, and protecting POS terminals to mitigate the risk of data breaches, fraud, and other security incidents. By implementing specific security measures tailored to the unique characteristics and requirements of POS systems, we can enhance our overall cybersecurity posture and ensure the integrity and confidentiality of customer data.

Title: Secure Usage Policy for Point-of-Sale (POS) Systems
Classification: Internal Use Only

Statement of Purpose

This policy addresses the secure and responsible usage of Point-of-Sale (POS) systems within the 4GuysCoffee enterprise. It encompasses hardware, software, and protocols associated with POS systems and is intended for authorised users within the organisation. Authorised users include employees, contractors, and vendors who are approved to access 4GuysCoffee's POS systems. All authorised users are expected to understand and adhere to the guidelines outlined in this policy.

Appropriate Use

POS systems will be used solely for processing transactions related to 4GuysCoffee's business operations. Only authorised personnel are permitted to access the POS terminals, and access should be restricted to individuals with a legitimate need for such access. Any use of POS systems for personal transactions or activities unrelated to 4GuysCoffee's business is strictly prohibited.

Systems Management

The IT department ensures all POS terminals' proper configuration and security. This includes maintaining up-to-date software patches, implementing robust authentication mechanisms, and monitoring suspicious activities or unauthorised access attempts. End-users are responsible for safeguarding their login credentials and immediately reporting any anomalies or security concerns related to POS systems to the IT department.

Data Protection

All transactions processed through the POS systems may contain sensitive customer information, including payment card data. Therefore, adhering to industry-standard data security practices, such as encryption of cardholder data during transmission and storage, compliance with Payment Card Industry Data Security Standards (PCI DSS), and regular security assessments and audits of POS systems.

Violations of Policy

Any unauthorised use, access, or manipulation of POS systems violates this policy. Violators may be subject to disciplinary action, up to and including termination of employment or contract, depending on the severity of the infraction. Suspected violations should be reported to the IT department or designated security officer for investigation and appropriate action.

Policy Review and Modification

This policy will be subject to periodic review by the IT department, with updates made as necessary to reflect changes in technology, regulations, or business requirements. Any modifications to the policy will be communicated to all relevant stakeholders, and training on updated procedures will be provided as needed.

Limitations of Liability

4GuysCoffee assumes no liability for unauthorised activities or security breaches resulting from the misuse or exploitation of POS systems. Any individuals found to have engaged in

such activities will be held personally liable, and 4GuysCoffee will cooperate fully with law enforcement authorities in prosecuting such individuals to the fullest extent permitted by law.

Systems-Specific Security Policy (SysSP):
Title: System and Software Security Policy (SysSP)
Classification: Internal Use Only

Statement of Purpose
The System and Software Security Policy (SysSP) aims to establish guidelines and procedures for ensuring the security and integrity of all systems and software used within the 4GuysCoffee. This policy applies to all employees, contractors, and third-party vendors who can access or interact with 4GuysCoffee's systems and software. Adherence to this policy is mandatory to protect sensitive information, maintain operational continuity, and mitigate cybersecurity risks.

Scope
This policy covers all aspects of system and software security, including but not limited to the following:

1. Installation and configuration of software applications and operating systems.
2. Access control measures to restrict unauthorised access to systems and software.
3. Regular software updates and patch management procedures.
4. Data backup and recovery processes to ensure data availability and resilience.
5. Incident response protocols for promptly addressing security breaches or vulnerabilities.
6. Compliance with legal and regulatory requirements governing system and software security.

Responsibilities
All employees, contractors, and third-party vendors are responsible for adhering to the guidelines outlined in the SysSP. Specific responsibilities include:

- System Administrators: Responsible for implementing and maintaining security measures for systems and software, including access controls, patch management, and regular system monitoring.
- End Users: Required to follow security best practices when using company systems and software, such as choosing strong passwords, avoiding unauthorised software installations, and reporting security incidents promptly.
- Information Security Team: Tasked with overseeing the implementation of the SysSP, conducting regular security assessments, and providing guidance and support to ensure compliance with security policies and procedures.

Security Controls

The SysSP defines the following security controls to protect systems and software from unauthorised access, data breaches, and other security threats:

- Access Control: Implement role-based access control (RBAC) to restrict access to sensitive systems and data based on users' roles and responsibilities.
- Encryption: Utilize encryption technologies to protect data at rest and in transit, ensuring confidentiality and integrity.
- Authentication: Enforce multi-factor authentication (MFA) for accessing critical systems and software, adding an extra layer of security.
- Patch Management: Establish procedures for regularly updating and patching software to address known vulnerabilities and mitigate security risks.
- Logging and Monitoring: Implement robust logging and monitoring mechanisms to detect and respond to security incidents in real time.
- Incident Response: Develop and maintain an incident response plan to guide the response and recovery process during a security breach or incident.

Violation of Policy

Any violation of the SysSP will result in disciplinary action, up to and including termination of employment or contract, as well as legal consequences if warranted. Employees must report any suspected violations of this policy to their immediate supervisor or the Information Security team for investigation and resolution.

Policy Review and Modification

The SysSP will be reviewed annually by the Information Security team to ensure its effectiveness and relevance in addressing emerging threats and technology changes. Modifications to the policy may be made as necessary to reflect updates in security best practices, regulatory requirements, or organisational changes.

Limitations of Liability

4GuysCoffee assumes no liability for unauthorised acts that violate local, state, or federal legislation. Employees are expected to comply with all applicable laws and regulations related to system and software security, and any violations will be subject to appropriate legal action.

This System and Software Security Policy (SysSP) is a cornerstone for maintaining the confidentiality, integrity, and availability of 4GuysCoffee's systems and software assets. All employees and stakeholders must understand and adhere to the guidelines to mitigate security risks and safeguard our organisation's information assets.

Incident Response Plan (IRP): At 4GuysCoffee, cybersecurity is a top priority, and the company has established measures to respond effectively to cyberattacks. While specific details of 4GuysCoffee's incident response plan may not be publicly available, we can draw

insights from industry best practices and past incidents to infer certain aspects of their approach.

In a cyberattack, 4GuysCoffee immediately mitigates the impact and protects its customers and business operations. For example, if a cyberattack were to compromise customer data or disrupt services, 4GuysCoffee would promptly notify affected customers through various communication channels, such as email or official announcements on its website. The company would provide clear and transparent information about the incident, including details on the nature of the attack, the data compromised, and steps customers can take to safeguard their information.

Prevention is a key focus area for 4GuysCoffee's cybersecurity strategy. The company proactively identifies and addresses common vulnerabilities and threats, such as application security flaws, phishing attacks, and misconfigurations of IT systems. By prioritising these areas for defensive measures, 4GuysCoffee aims to strengthen its overall cybersecurity posture and minimise the likelihood of successful cyberattacks. Additionally, 4GuysCoffee emphasises the importance of good password hygiene and advises customers to avoid reusing credentials across multiple platforms, reducing the risk of credential-based attacks.

Furthermore, 4GuysCoffee actively collaborates and shares information with other industry stakeholders to enhance its cybersecurity capabilities. By participating in forums, sharing insights from past incidents, and learning from the experiences of peers, 4GuysCoffee stays informed about emerging threats and trends in the cybersecurity landscape. This collaborative approach enables 4GuysCoffee to adapt its security practices proactively and respond effectively to evolving cyber threats.

1. Incident Response Team

   General Manager (GM): The GM oversees the incident response process and ensures it aligns with the organisation's objectives and priorities.

   Head of Technology (HOT): The HOT provides technical expertise and guidance on cybersecurity issues, assessing the technical aspects of security incidents and implementing measures to mitigate risks.

   Head of Human Resources (HOHR): The HOHR manages the impact of security incidents on employees, provides support and guidance throughout the incident response process, and ensures compliance with relevant employment laws and regulations.

   Head of Customer Service (HOCS): The HOCS assesses the impact of security incidents on customers, manages customer communications, and addresses customer-facing issues during incident response activities.

Head of Sales & Marketing (HOSM): The HOSM manages the reputation and public perception of the organisation during security incidents, develops communication strategies, and addresses potential reputational damage.

Head of Logistics (HOL): The HOL assesses the impact of security incidents on logistics and operations, identifies vulnerabilities in the supply chain, and implements measures to mitigate risks.

Head of Operations (HOO): The HOO oversees incident response activities related to the roasting facility and cafe operations, ensuring compliance with food safety regulations and industry standards.

2. Incident Response Process

I. Incident Identification and Reporting:

At 4GuysCoffee, the first step in our incident response plan is to ensure that all employees are adequately trained to recognise signs of a cybersecurity incident. This includes being vigilant for unusual system behaviour, suspicious emails, or unauthorised access attempts. Upon identifying a potential incident, employees must report it immediately to the designated incident response team or IT security personnel. This swift reporting ensures that incidents can be addressed promptly, minimising their impact on our business operations and customer data.

II. Initial Assessment and Triage:

Upon receiving a report of a potential cybersecurity incident, our incident response team conducts an initial assessment to determine the severity and potential impact of the incident. This assessment involves gathering information about the nature of the incident, the systems or data affected, and any potential vulnerabilities that may have been exploited. Based on this assessment, the incident is triaged to determine the appropriate response actions and escalation procedures. This ensures that resources are allocated effectively and that the incident response process is prioritised according to the level of risk posed to our organisation.

III. Containment and Mitigation:

Once the incident has been assessed, immediate steps are taken to contain the incident and prevent further damage or unauthorised access. This may involve isolating affected systems, deactivating compromised accounts, or implementing temporary security controls to mitigate the impact of the incident. Containment measures are crucial for minimising the spread of the incident and preventing it from escalating into a more significant security breach.

IV. Investigation and Analysis:
Following containment, a thorough investigation is conducted to determine the incident's root cause and understand how the attack occurred. This investigation involves analysing logs, examining system configurations, and performing forensic analysis to gather evidence. By understanding the tactics, techniques, and procedures the attackers use, we can better prepare our defences and prevent similar incidents.

V. Communication and Notification:
Transparent and timely communication is essential during a cybersecurity incident. We maintain open lines of communication with stakeholders, including customers, employees, regulatory authorities, and law enforcement agencies, as required by applicable laws and regulations. Affected parties are notified promptly, providing clear and accurate information about the incident and its impact and recommended actions to protect themselves. This proactive communication helps to build trust and confidence among our stakeholders and demonstrates our commitment to transparency and accountability.

VI. Recovery and Restoration:
Once the incident has been contained and investigated, efforts focus on restoring affected systems and data to their pre-incident state. This may involve leveraging backups to recover lost or corrupted data and implementing additional security measures to harden our systems against future attacks. The goal of the recovery phase is to minimise downtime, restore normal operations, and ensure the integrity and availability of our business-critical systems and data.

VII. Post-Incident Analysis and Lessons Learned:
After the incident has been resolved, a post-incident analysis is conducted to evaluate the effectiveness of our incident response process and identify areas for improvement. Lessons learned from the incident are documented and used to update policies, procedures, and security controls to enhance resilience and prevent future incidents. By continuously learning from our experiences and adapting our practices, we can strengthen our defences and better protect our organisation against cybersecurity threats.

VIII. Ongoing Monitoring and Improvement:
Finally, we recognise that cybersecurity is an ongoing process that requires continuous monitoring and improvement. We conduct regular reviews and exercises of our incident response plan to ensure readiness and effectiveness in responding to cybersecurity incidents. This proactive approach helps us avoid emerging threats, identify potential vulnerabilities, and continuously improve our incident response capabilities. By remaining vigilant and proactive, we can better protect our organisation and stakeholders from the ever-evolving landscape of cybersecurity threats.

Disaster Recovery Plan (DRP):

1. Introduction

   The Disaster Recovery Plan (DRP) for 4GuysCoffee outlines the procedures and protocols to restore critical IT systems and operations during a disaster or disruptive incident. The plan aims to minimise downtime, mitigate data loss, and ensure business continuity for 4GuysCoffee.

2. Risk Assessment

   Identification of Potential Risks: Potential risks include natural disasters like earthquakes and floods, cyberattacks like ransomware, hardware failures in servers or networking equipment, and human errors such as accidental data deletion.

   Impact Analysis: The impact of a disaster on critical IT systems, including the point of sale (POS) system, customer database, inventory management, and financial records, could result in prolonged downtime, data loss, revenue loss, and damage to the brand's reputation.

3. Business Impact Analysis (BIA)

   Identification of Critical Systems and Processes: Critical systems and processes include the POS system for sales transactions, the customer database for order history and loyalty programs, inventory management for stock control, and financial records for accounting and reporting purposes.

   Determine Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO): The RTO for critical systems is within 24 hours, ensuring minimal disruption to business operations. The RPO, such as daily backups, is set regularly to minimise data loss.

4. Disaster Recovery Strategies

   Backup and Recovery: Regular backups of critical data are performed daily and stored on-site and off-site, ensuring data availability for restoration. Automated backup solutions are in place to streamline the backup process.

   Failover and Redundancy: Redundant hardware components, such as servers and networking equipment, are deployed to provide failover capabilities and ensure the high availability of critical systems. Cloud-based services are used for redundancy and scalability.

Data Replication: Data replication technologies are utilised to maintain synchronised copies of critical data in geographically dispersed locations, providing resilience against data loss and ensuring data availability during a disaster.

5. Disaster Recovery Plan Implementation

Activation Procedures: The disaster recovery plan is activated upon detection of a critical system failure or declaration of a state of emergency by designated personnel. Emergency notification systems are in place to alert key stakeholders.

Emergency Response: Clear communication channels and escalation procedures are established to promptly notify key personnel and activate the disaster recovery team. Contact lists and emergency contact information are regularly updated.

Recovery Procedures: Step-by-step procedures are documented and readily accessible to the disaster recovery team. The responsibilities of team members are clearly defined, and timelines for completing recovery activities are established to ensure a swift restoration of services.

6. Testing and Training

Regular Testing: Regular disaster recovery drills and tabletop exercises are conducted to test the effectiveness of the DRP and identify any gaps or weaknesses. Feedback from drills is used to refine and improve the plan continuously.

Training and Awareness: Ongoing training and awareness programs are provided to educate employees on disaster recovery procedures, emergency response protocols, and the importance of business continuity planning. Training sessions are conducted regularly to ensure all employees are prepared to respond effectively to disasters.

7. Documentation and Review

Documentation: Detailed documentation of the disaster recovery plan, including recovery procedures, contact lists, system configurations, and test results, is maintained and regularly updated. Documentation is stored securely and accessible to authorised personnel.

Regular Review: The disaster recovery plan is reviewed and updated regularly to reflect technological changes, infrastructure, business processes, and emerging threats. Reviews are conducted annually or as necessitated by changes in the business environment.

8. Conclusion

The Disaster Recovery Plan is a critical component of 4GuysCoffee's resilience strategy, ensuring the organisation can recover from disruptive incidents and maintain business continuity. By implementing proactive measures, conducting regular testing, and fostering a culture of preparedness, 4GuysCoffee can minimise the impact of disasters and safeguard its operations and reputation.

Business Continuity Plan (BCP): The Business Continuity Plan (BCP) for 4GuysCoffee is a comprehensive strategy designed to ensure the organisation can maintain critical business functions and services during disruptions or emergencies. It outlines proactive measures, such as alternate work arrangements, redundancy systems, and supplier management, to minimise the impact of disruptions on operations and safeguard the organisation's reputation and financial stability. The BCP aims to enhance resilience and enable effective response and recovery efforts in the face of adversity through regular testing, training, and documentation.

Introduction

The Business Continuity Plan (BCP) for 4GuysCoffee outlines the strategies and procedures to ensure the continued delivery of critical business functions and services during disruptions or emergencies. The plan aims to minimise the impact of disruptions, maintain customer service levels, and safeguard the reputation and financial stability of 4GuysCoffee.

Risk Assessment

Identification of Potential Risks: Potential risks include natural disasters such as floods, as well as human-made threats like cyberattacks, infrastructure failures, and supply chain disruptions.

Impact Analysis: The impact of a disruption on critical business functions, including sales operations, customer service, supply chain management, and financial transactions, could result in revenue loss, customer dissatisfaction, reputational damage, and regulatory non-compliance.

Business Impact Analysis (BIA)

Identification of Critical Business Functions: Critical business functions include sales processing, customer support, inventory management, financial transactions, and marketing communications. These functions are essential for maintaining business operations and meeting customer demands.

Determine Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO): The RTO for critical business functions is within 24 to 48 hours, ensuring minimal disruption to operations. The RPO, such as daily backups, is set regularly to minimise data loss and ensure data integrity.

Business Continuity Strategies

Alternate Work Arrangements: Remote work arrangements are established to allow employees to work from home or other off-site locations in the event of office closures or travel restrictions. Virtual collaboration tools and secure remote access solutions are deployed to facilitate remote work.

Redundancy and Backup Systems: Redundant systems and backup solutions are implemented to ensure the availability of critical IT systems and data. Backup servers, cloud-based services, and data replication technologies are utilised to maintain redundancy and data integrity.

Supplier and Vendor Management: Relationships with key suppliers and vendors are managed proactively to mitigate supply chain disruptions. Alternative suppliers and vendors are identified, and contingency plans are developed to ensure the availability of essential goods and services.

Business Continuity Plan Implementation

Activation Procedures: The BCP is activated upon a disruptive incident or emergency. Designated personnel are responsible for initiating the BCP activation process and notifying key stakeholders and response teams.

Emergency Response: Emergency response teams are mobilised promptly to assess the situation, implement response measures, and coordinate recovery efforts. Clear communication channels and escalation procedures are established to ensure effective communication and decision-making.

Continuity of Operations: Critical business functions are prioritised for continuity, and alternative work arrangements are implemented to ensure the ongoing delivery of services to customers. Regular updates and communication with employees, customers, and stakeholders are provided to maintain transparency and trust.

Testing and Training

BCP Testing: Regular testing and exercises of the BCP are conducted to evaluate its effectiveness and identify areas for improvement. Tabletop exercises, simulation drills, and scenario-based training sessions are conducted to familiarise employees with their roles and responsibilities during a crisis.

Employee Training: Ongoing training and awareness programs are provided to educate employees on the BCP, emergency response procedures, and crisis management protocols. Training sessions cover evacuation procedures, communication protocols, and business continuity best practices.

Documentation and Review

Documentation: Detailed documentation of the BCP, including procedures, contact lists, recovery plans, and test results, is maintained and regularly updated. Documentation is stored securely and accessible to authorised personnel.

Regular Review: The BCP is reviewed and updated regularly to reflect changes in business operations, technology, regulatory requirements, and emerging threats. Reviews are conducted annually or as necessitated by changes in the business environment.

Conclusion

The Business Continuity Plan is a critical component of 4GuysCoffee's resilience strategy, ensuring the organisation can withstand and recover from disruptions effectively. By implementing proactive measures, conducting regular testing and training, and maintaining clear communication channels, 4GuysCoffee can minimise the impact of emergencies and maintain business continuity, even in challenging circumstances.

GRC Conclusion

In conclusion, the Governance, Risk, and Compliance (GRC) report encapsulates a comprehensive overview of 4GuysCoffee's commitment to mitigating risks and upholding regulatory standards in an ever-evolving digital environment. Key findings underscore the imperative for robust information security measures, as highlighted by identifying vulnerabilities such as unpatched bugs and weak web applications. Implementing strategic security controls, including role-based access control, encryption, and incident response protocols, demonstrates our proactive stance in protecting sensitive data and preserving customer trust. Furthermore, the positive cost-benefit analysis explored in the report exemplifies the tangible benefits of investing in cybersecurity measures. Leveraging innovative solutions such as Docker on AWS Linux to host our Security Information and Event Management (SIEM) system underscores our commitment to enhancing security capabilities while optimising cost-effectiveness. Moreover, adopting a Learning Management System underscores our recognition of the human element in cybersecurity, empowering employees through continuous education and reinforcing a security-conscious culture. As we navigate the intricacies of the digital landscape, our unwavering dedication to responsible data

stewardship and resilience against cyber threats ensures our stakeholders' continued success and trust.

Capstone Conclusion

Over the past six months, our team has conducted a comprehensive evaluation of 4GuysCoffee's business operations, focusing on its IT infrastructure. Through this evaluation, we identified areas for improvement and proposed a new infrastructure solution designed to address current challenges and accommodate future growth.

One of the key enhancements we introduced was the deployment of state-of-the-art Cisco switches and routers. These devices were strategically placed throughout the organization to ensure seamless connectivity and robust network performance.

Additionally, we implemented a Windows Active Directory (AD) system for 4GuysCoffee. This centralized directory service allows for the efficient management and organization of users and resources across the entire organization, streamlining administrative tasks and enhancing security.

Recognising the importance of establishing an online presence, we launched the 4GuysCoffee website on an AWS instance. This move enables the company to expand its reach and sell products online to customers worldwide, driving growth and revenue opportunities.

In response to the SQL injection attack on 4GuysCoffee's network, our team conducted thorough forensic analysis to understand the attack vectors and vulnerabilities exploited by the attacker. We began by examining server logs and database records to trace the origin of the malicious SQL queries and identify any unauthorized access points. Additionally, we utilised specialised forensic tools to analyze network traffic patterns and identify anomalies indicative of the attack. Through meticulous examination of system artifacts and event logs, we were able to reconstruct the timeline of the attack and gather critical evidence to inform our mitigation strategy and strengthen the network's defenses against future intrusions.

As part of our security enhancement efforts, we implemented a robust Next-Gen Firewall solution provided by Palo Alto Networks. This firewall is designed to prevent unauthorized access to resources and safeguard inbound and outbound network traffic, ensuring the integrity and confidentiality of data.

Furthermore, we deployed a Security Incident and Events Management (SIEM) tool by Wazuh. This advanced monitoring system continuously monitors network activity and alerts administrators to any suspicious or unauthorized access attempts, enabling timely response and mitigation of potential security threats.

To ensure compliance with governance, risk, and compliance (GRC) standards, we provided 4GuysCoffee with a comprehensive compliance framework tailored to their specific regulatory requirements, including PDPA and PCIDSS. This framework includes detailed policies and procedures that employees must adhere to, promoting a culture of compliance and security awareness throughout the organization.

Team Member Contributions

	Team Member Full Name	List all the contributions of the team member towards this project
1	Koh Jun Kai Brendan	• M3 • M4 • M5 • M6 • M7 • M8
2	Muhammad Shafeeq Bin Abdul Talib	• M2 • M4 • M5 • M6 • M7 • M8
3	Muhammad Hud Bin Ayub	• M1 • M2 • M4 • M5 • M6 • M7 • M8

References

1. Lau, Deborah. “The Big Read in Short: What’s Driving Singapore’s Coffee Craze?” TODAY, November 4, 2023. https://www.todayonline.com/big-read/big-read-short-whats-driving-singapores-coffee-craze-2297136
2. “Hierarchical Network Design.” GeeksforGeeks, November 17, 2022. https://www.geeksforgeeks.org/hierarchical-network-design/
3. IP addressing guide - Cisco. Accessed January 14, 2024. https://www.cisco.com/c/dam/global/en_ca/solutions/strategy/docs/sbaBN_IPv4addrG.pdf
4. What is Amazon EC2? - Amazon Elastic Compute Cloud. Accessed January 14, 2024. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html
5. Canadian Centre for Cyber Security, Canadian Centre for Cyber Security (Cyber Centre). “Practitioner Guidance for Securing Microsoft Active Directory Services in Your Organization.” ITSP.60.100, December 12, 2023. https://www.cyber.gc.ca/en/guidance/practitioner-guidance-securing-microsoft-active-directory-services-your-organization-itsp60100
6. Microsoft. Group Policy Management Console, May 31, 2018. https://learn.microsoft.com/en-us/previous-versions/windows/desktop/gpmc/group-policy-management-console-portal
7. Microsoft. “The Active Directory Module with PowerShell.” ActiveDirectory. Accessed January 14, 2024. https://learn.microsoft.com/en-us/powershell/module/activedirectory/?view=windowsserver2022-ps
8. Microsoft. “Understanding The Active Directory Logical Model.” Microsoft Learn, July 30, 2021. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model#active-directory-organizational-units
9. “Reasons Why the Demand for Specialty Coffee Is Growing This Year.” Groundwork Coffee Co. Accessed January 14, 2024. https://www.groundworkcoffee.com/blogs/learn/top-reasons-why-the-demand-for-specialty-coffee-is-growing-this-year
10. “Biannual Threats Report - Visa.” Visa, June 2022. https://usa.visa.com/content/dam/VCOM/regional/na/us/run-your-business/documents/biannual-threats-report.pdf
11. Allied Market Research. Rep. Digital Payment Market Size, Share, Competitive Landscape and Trend Analysis Report. Global Opportunity Analysis and Industry Forecast. Allied Market Research, 2023.
12. DXC Technology. “As Online Shopping Grows, So Does The Risk of e-Skimming Attacks,” n.d.
13. Lvovsky, Roman. 2023. Review of The Art of Concealment: A New Magecart Campaign That’s Abusing 404 Pages. Akamai Security Intelligence. https://www.akamai.com/blog/security-research/magecart-new-technique-404-pages-skimmer
14. PERSONAL DATA PROTECTION COMMISSION, 2023. SGPDPC 10, Case No. DP-2209-C0193 / DP-2209-C0217.

https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/GD_Ascentis_12092023.pdf
15. Anderson, R., Ponant, & Audette, J. (2019, November 3). Account confirmation and password recovery in ASP.NET Core. Retrieved from Microsoft: https://docs.microsoft.com/en-us/aspnet/core/security/authentication/accconfirm?view=aspnetcore-5.0&tabs=visual-studio
16. IBM Cloud Education. (2020, October 28). Three-Tier Architecture. Retrieved from IBM: https://www.ibm.com/sg-en/cloud/learn/three-tier-architecture
17. SFA. SFA, March 27, 2024. https://www.sfa.gov.sg/docs/default-source/food-farming/coastal_farm_personnel.pdf
18. "CVE-2023-26369." CVE. Accessed April 5, 2024. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26369
19. Petrosyan, Ani. "Annual Number of Supply Chain Cyber Attacks U.S. 2023." Statista, March 26, 2024. https://www.statista.com/statistics/1367208/us-annual-number-of-entities-impacted-supply-chain-attacks/
20. PCI DSS v3.2.1 quick reference guide, July 2018. https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf
21. Wolford, Ben. "What Is GDPR, the EU's New Data Protection Law?" GDPR.eu, September 14, 2023. https://gdpr.eu/what-is-gdpr/
22. "PDPC: PDPA Overview." Personal Data Protection Commission. Accessed April 10, 2024. https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act
23. Kaspersky. "What Is Security Awareness Training?" www.kaspersky.com, December 8, 2023. https://www.kaspersky.com/resource-center/definitions/what-is-security-awareness-training
24. Kirvan, Paul. "Incident Response Plan: How to Build, Examples, Template." Security, January 22, 2024. https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan#:~:text=Incident%20response%20plans%20help%20reduce,the%20event%20of%20an%20incident
25. Aijaz, Shigraf. "Incident Response Team." AT&T Cybersecurity, 10AD. https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/arming-your-incident-response-team
26. Schneier, Bruce. "The Future of Incident Response." Schneier on security, November 10, 2014. https://www.schneier.com/blog/archives/2014/11/the_future_of_i.html
27. Knapp, Kenneth J., ed. 2009. Cyber-Security and Global Information Assurance : Threat Analysis and Response Solutions. Hershey, Pa: IGI Global. https://doi.org/10.4018/978-1-60566-326-5
28. Paarlberg, Jon W. 2016. "An Empirical Analysis on the Effectiveness of Information Security Policies, Information Technology Governance, and International Organization for Standardization Security Certification." ProQuest Dissertations Publishing
29. AlGhamdi, Sultan, Khin Than Win, and Elena Vlahu-Gjorgievska. 2020. "Information Security Governance Challenges and Critical Success Factors: Systematic Review." Computers & Security 99: 102030-. https://doi.org/10.1016/j.cose.2020.102030
30. Santos, Omar. 2015. The Current Security Threat Landscape Networking Talks LiveLessons. 1st edition. Cisco Press

31. Lagana, Matthew. 2018. “Information Security in an Ever-Changing Threat Landscape.” In The Routledge Companion to Risk, Crisis and Security in Business, 1st ed., 255–71. Routledge. https://doi.org/10.4324/9781315629520-17
32. RSI Security. “What Is the Purpose of an Enterprise Information Security Policy?” RSI Security, April 5, 2019. https://blog.rsisecurity.com/what-is-the-purpose-of-an-enterprise-information-security-policy/
33. “Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook.” NIST SP 800-12: Chapter 5 - Computer Security Policy, July 25, 2014. https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter5.html
34. Heymsfeld, Ralph. “Security Policy Framework.” CertMike, August 30, 2018. https://www.certmike.com/security-policy-framework/
35. Gihon, Shmuel. “Ransomware Trends 2023 Report.” Cyberint, April 7, 2024. https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/#:~:text=In%20the%20year%202022%2C%20a,substantial%20increase%20of%20%3E55%25
36. Acunetix. “What Is SQL Injection (Sqli) and How to Prevent Attacks.” Acunetix, January 9, 2024. https://www.acunetix.com/websitesecurity/sql-injection/
37. “Cost of a Data Breach 2023.” IBM. Accessed April 15, 2024. https://www.ibm.com/reports/data-breach
38. “Cybercrime Thrives during Pandemic: Verizon 2021 Data Breach Investigations Report.” Verizon, May 20, 2021. https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report
39. Check Point Software. “2021 Cyber Security Report.” Check Point Software, July 21, 2021. https://www.checkpoint.com/pages/cyber-security-report-2021/