

ICT171 Assignment 2

Documentation



June 1, 2025

Murdoch Universtty

Name: Jigme Kuendrol Wangchuk || student ID: 35479911

# Project Overview:

The purpose of this project is to launch a cybersecurity awareness blog server online using IAAS on an Ubuntu EC2 AWS instance. The main purpose of creating this blog is to show people the importance of cybersecurity, along with providing users with a reliable blog website that is secure and easily accessible. The project also includes setting up the server, hosting the content, securing it with SSL, and assigning a custom domain name. It is intended to remain live and be expandable for future development.

# Server:

## AWS EC2 Instance:

1. Region: US East (N. Virginia) us-east-1c (Amazon Web Services, n.d)
2. Instance Type: t2.micro (Amazon Web Services, n.d)
3. IP address: Elastic IP has been purchased and allocated to the instance
4. Security: HTTPS access was enabled using an SSL certificate from Let’s Encrypt, which ensured the transfer of safe traffic only.

A screenshot of a computer

AI-generated content may be incorrect.

# Deployment of Website:

## Apache 2 Web Server Setup:

1. Created an AWS EC2 (Ubuntu) instance online and launched it (Amazon Web Services, n.d)
2. Save the ssh file in a safe place
3. Configure the instance with an Elastic IP in the Elastic IP options
4. Go to PowerShell and log in to the files where the documents(SSH) are saved
5. log in to the Ubuntu server by using the command: “ssh -i JiggysSecurity.pem ubuntu@<[52.73.48.19](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ElasticIpDetails:PublicIp=52.73.48.19)>”
6. Installed Apache2: “sudo apt update && sudo apt install apache2 ”
7. Uploaded files through scp: scp index.html ubuntu@<[52.73.48.19](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ElasticIpDetails:PublicIp=52.73.48.19)>:/var/www/html/
8. Verified if the site loads using the elastic IP

A screenshot of a computer screen

AI-generated content may be incorrect.

## Linking DNS:

1. Go to an online domain name provider like name cheap
2. Domain provider: namecheap (Namecheap, n.d)
3. Once we are on the website (Namecheap), purchase a DNS relevant to our topic
4. Domain name: cyberawareblog.org
5. Once the domain name is purchased, link it to our instance
6. Linked DNS to the instance using Elastic IP

A screenshot of a computer

AI-generated content may be incorrect.

## SSL configuration:

Used Let’s Encrypt to enable HTTPS (Let’s Encrypt, 2024)

1. Open Ubuntu and login to our server using the command “ssh -i (key\_name) ubuntu@<elastic IP>”
2. Firstly, perform the commands: sudo apt update and apt install apache2 to make Apache ready for installation as it updates the package and also install Apache
3. Installed Certbot: “sudo apt install certbot python3-certbot-apache”
4. Ran: “sudo certbot –apache”
5. SSL certificate successfully installed

A screenshot of a computer screen

AI-generated content may be incorrect.

## Website editing:

1. Once logged into the server, use the command: scp index.html ubuntu@<Elastic IP>:/var/www/html/ to edit the server designs and content.
2. Make necessary changes to the website content using HTML and CSS.
3. W3Schools provides the necessary coding information to create designs.
4. After editing, save the work and exit.

A screenshot of a computer screen

AI-generated content may be incorrect.

# Script Summary:

## Script:

File name: security\_script.sh

sudo apt update: makes Apache ready for installation as it updates the package

sudo apt install apache2 : installs apache

sudo ufw enable: enables the firewall for the server

sudo apt install certbot python3-certbot-apache : installs certbot for ssl certificate

sudo certbot - -apache: Runs Certbot to configure Apache with the SSL certificate

## Explanation:

This script updates the server, installs Apache2, installs Certbot, enables the firewall, and runs SSL setup. This makes server deployment secure and easily accessible.

## Maintenance Considerations:

For the server to run and last for multiple years:

1. Cost: EC2 ($11.95/month) + domain ($1.25/month) + data transfer(In-free, out-$0.09 after 15GB limit) (Amazon Web Services, n.d)
2. Storage: EBS for larger storage
3. SSL: Let’s Encrypt provides auto-renewals (Let’s Encrypt, 2024)
4. Updates: Regularly run updates to maintain security

## GitHub Timeline Evidence:

A screenshot of a computer

AI-generated content may be incorrect.

## Conclusion:

This project taught me how to launch and configure a cloud server using AWS EC2(IAAS), deploy and secure a website, and connect it to a DNS. I learned about IaaS pricing, DNS configuration, SSL installation, and writing scripts. In the future, I plan on expanding this blog with the new skills I’ll be learning as I continue to grow my knowledge during my time at university and after.

## Licensing:

The licensing used was Creative Commons (CC-BY 4.0) as it allows users to build on my work as long as the attribution is given to the creator. (Credit must be given to the creator.)

## Information:

1. Site: <https://cyberawareblog.org>
2. GitHub: <https://github.com/Jiggy-cyber/ICT171_Assignment2>
3. AWS region: US East (N. Virginia) us-east-1c
4. Instance type: t2.micro ((Amazon Web Services, n.d)
5. DNS provider: Namecheap (Namecheap, n.d)
6. SSL provider: Let’s Encrypt (Let’s Encrypt, 2024)

## References:

1. Let’s Encrypt. (2024). About Let’s Encrypt. <https://letsencrypt.org/about/>
2. Namecheap. (n.d). Domain Prices. <https://www.namecheap.com/domains/>
3. Amazon Web Services. (n.d). Amazon EC2. <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Overview>:
4. Creatve Commons.(n.d).Attribution 4.0 International. <https://creativecommons.org/licenses/by/4.0/>