

COHORT-5

# CYBER SECURITY

O S I N T & V U L N E R A B I L I T Y M A N A G E M E N T



# INTRODUCTION

Name: Arslan Ali

Qualification: Software Engineering

Instructor: Sir Shahzaib Ali Khan

Course: Cybersecurity

Cohort: 5

# CYBERSECURITY

## PROJECT # 1

Open-source intelligence  
OSINT



## PROJECT # 2

Vulnerability Management  
Nessus Tool





# **PROJECT # 1**

## **OPEN-SOURCE INTELLIGENCE (OSINT)**

- Which company this IP belongs 54.239.28.85?
- What is the manufacturing date of this container? (Month and year only)
- In which country this image is most likely taken?
- In which country is this vehicle registered?
- Where did this plane land last as seen in the picture? Name of place?

# SPECIAL PERFORM IN CONCERT



who.is Search for domains or IP addresses...

Premium

## IP Whois

NetRange: 54.224.0.0 - 54.255.255.255  
CIDR: 54.224.0.0/11  
NetName: AMAZON-2011L  
NetHandle: NET-54-224-0-0-1  
Parent: NET54 (NET-54-0-0-0-0)  
NetType: Direct Allocation  
OriginAS: AS16509  
Organization: Amazon Technologies Inc. (AT-88-Z)  
RegDate: 2012-03-01  
Updated: 2021-02-10  
Comment: -----BEGIN CERTIFICATE-----MIICljCCAX4CCQDvS1je18d4uzANB  
Ref: https://rdap.arin.net/registry/ip/54.224.0.0

OrgName: Amazon Technologies Inc.  
OrgId: AT-88-Z  
Address: 410 Terry Ave N.  
City: Seattle  
StateProv: WA  
PostalCode: 98109  
Country: US  
RegDate: 2011-12-08  
Updated: 2022-09-30  
Comment: All abuse reports MUST include:  
Comment: \* src IP  
Comment: \* dest IP (your IP)  
Comment: \* dest port



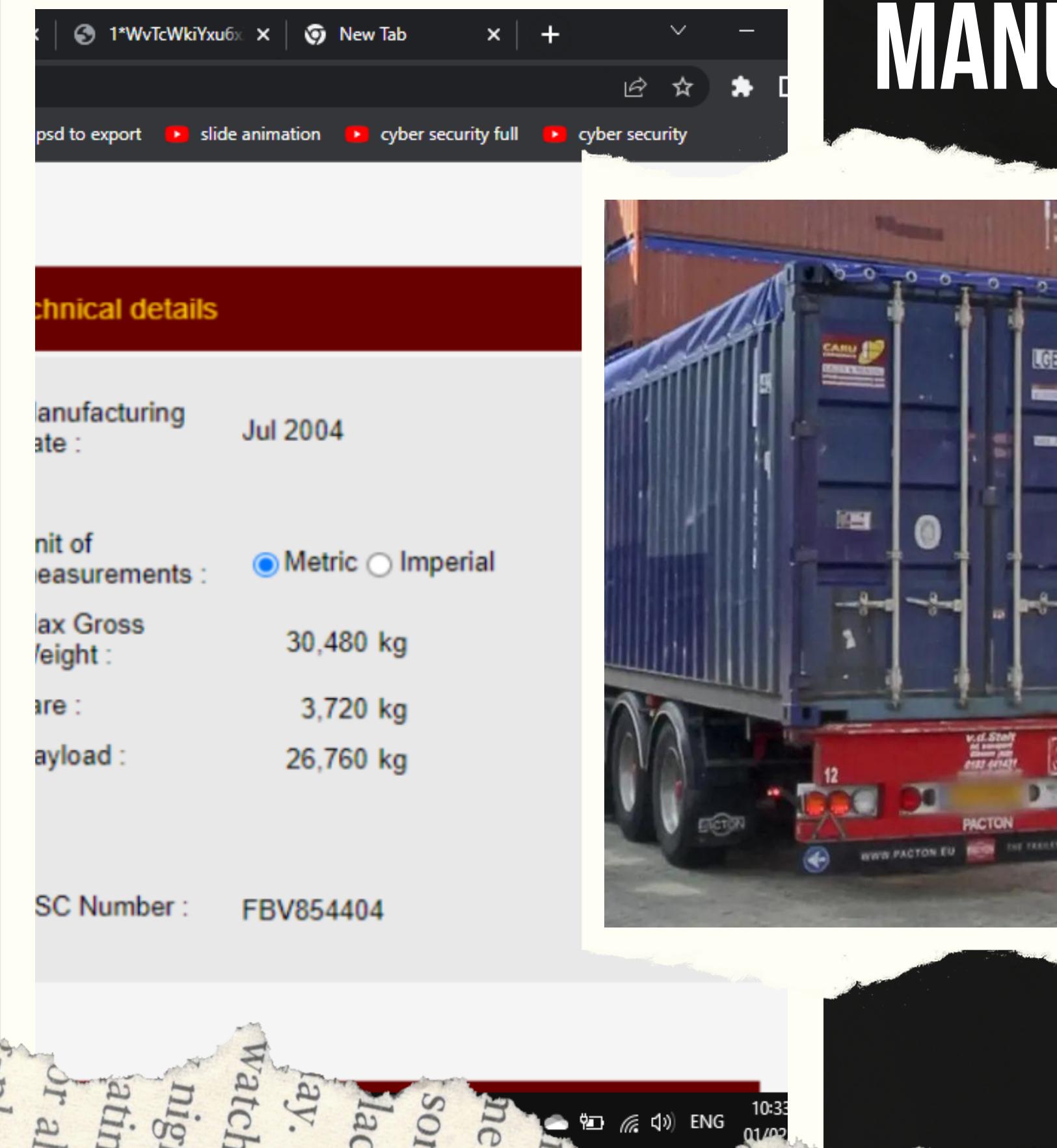
## WHO.IS

IP 54.239.28.85 belongs to  
**"Amazon Technologies Inc"**

## Google lens & Google Transale

Tayler shop in "**Dhaka**" which is  
the capital of **Bangladesh**.

# MANUFACTURING DATE OF CONTAINER



A screenshot of a web browser window. The title bar shows tabs for "1\*WvTcWkiYxu6x" (active), "New Tab", and "cyber security full". Below the tabs, there are links for "psd to export", "slide animation", "cyber security full", and "cyber security". The main content area has a red header bar with the text "Technical details". Below this, under "Manufacturing date", it says "Jul 2004". There are two radio buttons for "Unit of measurements": "Metric" (selected) and "Imperial". Other data listed include: Max Gross Weight: 30,480 kg, Axle: 3,720 kg, Payload: 26,760 kg, and SC Number: FBV854404. A photograph of a blue shipping container is visible on the right side of the page.

**"JULY 2004"**

**Container Tracking Number:**

LGEU 441697 3

**Container Company:**

CARU



**alltrack.org**



PLANE LAND LAST AS SEEN ?

"HUDSON RIVER" &  
CAROLINAS AVIATION MUSEUM

Name of plane  
"U.S. Airways Airbus A320 N106US "

Simple google search



thisdayinaviation.com



# COUNTRY OF VEHICLE

## "MOROCCO"

- Car name Dacia Dokker
- Limited Countries
- Match Number Plates



wikipedia



world licence plates.com

# PROJECT # 2

## VULNERABILITY MANAGEMENT

Demo Organization: <http://testphp.vulnweb.com/>

NESSUS SCAN



# HOW TO DOWNLOAD & SCAN WITH NESSUS

- 1 Go to Nessus web site and fill a form get the key
- 2 Download and Install Nessus for Window / Kali
- 3 Download and Install Nessus for Window / Kali
- 4 When Nessus open click on "Basic Network Scan" pate the demo site link and press lunch
- 5 It takes some time and the report will be generated by nessus .

# NESSUS REPORT

new site

Tue, 17 Jan 2023 16:11:46 Pakistan Standard Time

## TABLE OF CONTENTS

**Vulnerabilities by Host**

- [testphp.vulnweb.com](#)

**Vulnerabilities by Host**

[Collapse All](#) | [Expand All](#)

**testphp.vulnweb.com**

1	14	18	2	32
---	----	----	---	----

Severity	CVSS v3.0	Plugin	Name
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	8.3	42424	CGI Generic SQL Injection (blind)
HIGH	7.5	17797	PHP 5.x < 5.2.2 Multiple vulnerabilities
HIGH	7.5	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.3	25368	PHP < 5.2.3 Multiple Vulnerabilities
HIGH	7.5*	11139	CGI Generic SQL Injection
HIGH	7.5*	42479	CGI Generic SQL Injection (2nd pass)
HIGH	7.5*	35043	PHP 5 < 5.2.7 Multiple Vulnerabilities
HIGH	7.5*	31649	PHP 5.x < 5.2 Multiple Vulnerabilities
HIGH	7.5*	24907	PHP < 5.2.1 Multiple Vulnerabilities
HIGH	7.5*	41014	PHP < 5.2.11 Multiple Vulnerabilities
HIGH	7.5*	32123	PHP < 5.2.6 Multiple Vulnerabilities
HIGH	7.5*	35067	PHP < 5.2.8 Multiple Vulnerabilities



**THANK'S FOR WATCHING**

