

AWS EC2 Instance Port Scanner

Author: Daniel Chisasura

Version: 1.0

Purpose:

This script retrieves the public IP address of an AWS EC2 instance and performs a port scan using `nmap` to identify open services and potential vulnerabilities.

Overview

This Bash script is designed to help cloud administrators or security analysts quickly assess the network exposure of an EC2 instance. By automating the retrieval of the instance's public IP and scanning it with `nmap`, it provides a fast way to check for open ports and running services.


Prerequisites


- **AWS CLI:** Must be installed and configured (`aws configure`).
- **IAM Permissions:** Your IAM user or role must have permission to run `ec2:DescribeInstances`.
- **nmap:** Must be installed on your system.


Usage

1. **Make the script executable:** `chmod +x ec2_port_scanner.sh`
2. **Run the script with an EC2 instance ID:**
`./ec2_port_scanner.sh i-0123456789abcdef0`

Sample Output

 Retrieving Public IP for instance: i-0123456789abcdef0

 Public IP found: 203.0.113.25


 Starting nmap scan on 203.0.113.25...

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
--------	------	-----	--

80/tcp	open	http	Apache httpd 2.4.29 ((Ubuntu))
--------	------	------	--------------------------------

...

 Nmap scan complete.