# Nmap Detection and Scanning Report

Maya Lotfy

## 1. Introduction

This report provides a detailed account of the Nmap scanning performed on **[bWAPP "a buggy web application", Url: itsecgames.com ]**. The objective of the scan was to detect open ports, services, and potential vulnerabilities associated with the target. This scan is part of an ongoing security assessment to identify and address potential risks.

## 2. Objective

The primary objectives of the Nmap scan were to:

- Identify open ports on the target system.
- Detect the services and their versions running on these ports.
- Assess potential vulnerabilities that could be exploited by malicious actors.

## 3. Tools and Techniques Used

- **Tool**: Nmap (Network Mapper)
- **Version**: [7.94SVN]
- **Command Executed**: The following Nmap command was used for the scan:

## Scan Results

### 4.1. Summary of Findings

The scan results for `itsecgames.com` are as follows:

- **Host Information**:
  - **IP Address**: 31.3.96.40
  - **Reverse DNS Record**: web.mmebvba.com
- **Open Ports**:
  - **Port 22/tcp**: SSH (Secure Shell) - Used for secure command-line access.
  - **Port 80/tcp**: HTTP (Hypertext Transfer Protocol) - Used for serving web pages.
  - **Port 443/tcp**: HTTPS (Hypertext Transfer Protocol Secure) - Used for secure web traffic.

**Open Ports and Services**:

- **Port 22/tcp**:
  - **Service**: SSH

    - **Version**: OpenSSH 6.7p1 (protocol 2.0)
- **Port 80/tcp**:
    - **Service**: HTTP
    - **Version**: Apache HTTPD
- **Port 443/tcp**:
    - **Service**: HTTPS (SSL/HTTP)
    - **Version**: Apache HTTPD
- **Port States**:
    - **Port 22/tcp**: Open
    - **Port 80/tcp**: Open
    - **Port 443/tcp**: Open
- **Filtered Ports**:
    - The scan detected that 997 TCP ports are filtered and did not respond to the scan requests. This typically indicates that these ports are either blocked by a firewall or not listening.

### 4.2. Detailed Findings

| Port | Protocol | State | Service | Version |
|---|---|---|---|---|
| 22 | tcp | open | ssh | OpenSSH 6.7p1 |
| 80 | tcp | open | http | Apache HTTPD |
| 443 | tcp | open | ssl/http | Apache HTTPD |

## 5. Analysis

- **Open Ports and Services**:
    - **Port 22 (SSH)**: The SSH service is running OpenSSH 6.7p1. This version is relatively old, and there may be known vulnerabilities associated with it. Regular updates and security patches should be applied.
    - **Port 80 (HTTP)**: The HTTP service is provided by Apache HTTPD. The specific version was not identified, but it's important to ensure that this service is up to date to protect against known vulnerabilities.

    - **Port 443 (HTTPS)**: The HTTPS service is also provided by Apache HTTPD. The presence of SSL/TLS suggests that the service is configured to handle secure communications. Ensure that the SSL/TLS configurations are up to date and secure.
- **Filtered Ports**: The large number of filtered ports indicates a security mechanism, such as a firewall, that restricts visibility and access. This helps to mitigate the risk of exploitation by hiding non-essential services.

## 6. Recommendations

1. **Security Review**: Conduct a detailed security review of the services running on the open ports (SSH, HTTP, HTTPS) to ensure they are properly secured and configured.
2. **Firewall Configuration**: Review and update firewall rules to ensure that only necessary ports are open and accessible, reducing the potential attack surface.
3. **Service Hardening**: Ensure that the SSH service is configured with strong authentication methods, and that web services are protected against common vulnerabilities.
4. **Service Updates**:
    a. **OpenSSH**: Upgrade OpenSSH to a more recent version to mitigate known vulnerabilities and enhance security.
    b. **Apache HTTPD**: Ensure that Apache HTTPD is updated to the latest stable version. Regularly review and apply security patches.
5. **SSL/TLS Configuration**:
    a. Review the SSL/TLS configurations on the HTTPS service to ensure that they adhere to best practices. This includes using strong ciphers and protocols, and ensuring that SSL/TLS certificates are up to date.
6. **Firewall and Access Control**:
    a. Continue using firewalls to filter and manage network traffic. Regularly review firewall rules to ensure that they are effective and up to date.
7. **Regular Security Assessments**:
    a. Conduct regular security assessments and vulnerability scans to identify and address potential security issues proactively