Vulnerabilities and Countermeasures

Miguel Frade – Nuno Rasteiro

Department of Informatics Engineering
School of Technology and Management, Polytechnic Institute of Leiria

September 2019

Introduction

- The security issues we saw earlier are the product of the protocol specifications
- However there are more serious security issues that can affect any service, whether or not they have been specified with security as their primary purpose
- These problems are named as Vulnerabilities

Vulnerabilities

- What are Vulnerabilities
  - They are security flaws related or caused by implementation (programming) errors.
- What problems it can cause?
  - It depends, however the most serious one ones can allow an attacker to execute code and control the system
  - Imagine that, for example Amazon ecommerce platform, has these type of flaws
    - An attacker may access and steel all of the customers credit card numbers
    - The limit of the invasion is limited to the imagination and the will of the attacker

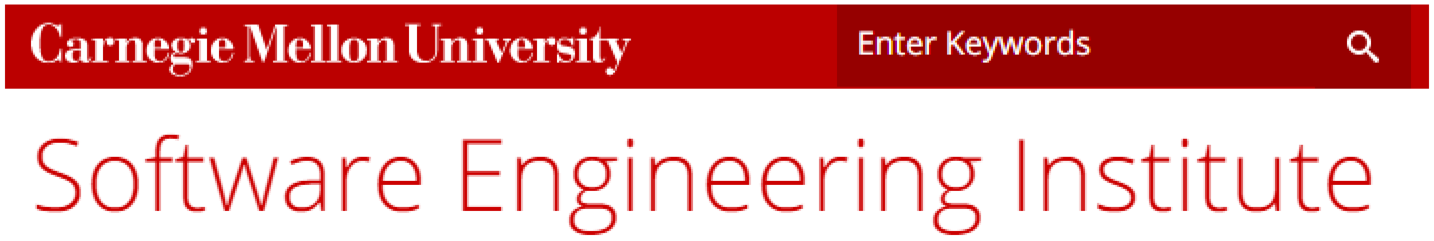
Vulnerabilities

- There are several organizations that record and describe the vulnerabilities found
  - Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org/
  - What is the main purpose of this site?

Common Vulnerabilities and Exposures

Search CVE List

  - CERT/CC:https://www.sei.cmu.edu/about/divisions/cert/index.cfm



Carnegie Mellon University

Enter Keywords

Software Engineering Institute

Vulnerabilities

- How can we detect if are systems have vulnerabilities
  - There are several applications (commercial and open source) that can perform automatic detection, called scanners of vulnerabilities
  - These applications depend on a database with all known vulnerabilities
  - These databases need to be updated regularly
- Examples of this type of application
  - Nessus: https://www.tenable.com/products/nessus
  - OpenVas: http://www.openvas.org/

nessus
Essentials

OpenVAS
Open Vulnerability Assessment Scanner

Nessus

- How does it work
  - Client server model
    - The server
      - Only exists in Linux
      - It does not have graphical interface
      - It is responsible to sent the probe packages and client management
    - The Client
      - Exists in Linux and Windows
      - Configurations are made on the graphical interface
      - This model has the advantage of only the server needs root access, the client can be executed by a normal user

OpenVAS

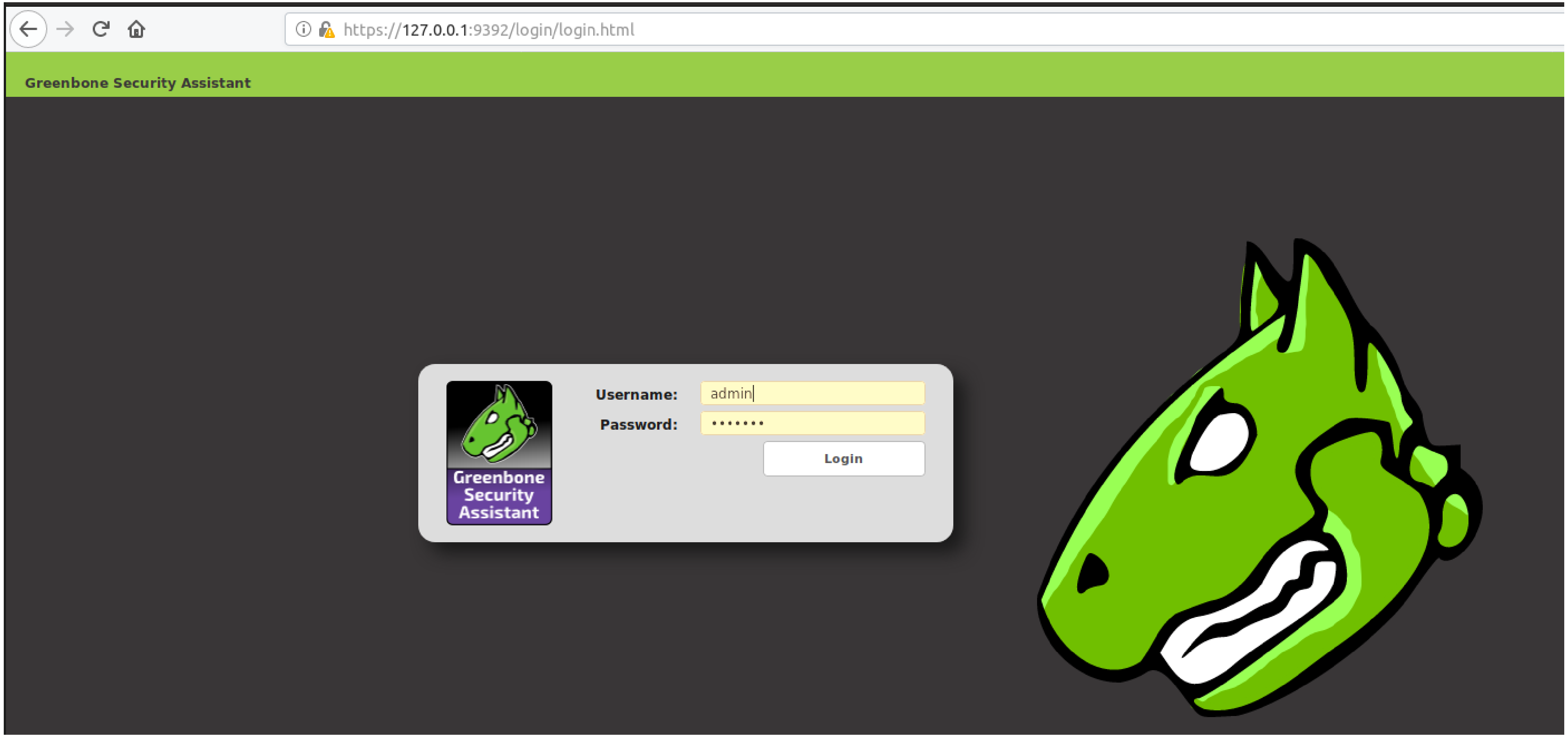
- OpenVAS – Open Vulnerability Assessment Scanner
  - Open Source Full-Featured vulnerability scanner
  - Includes more than 50000 vulnerability tests
  - Includes authenticated and unauthenticated testing
  - High level and low-level internet and industrial protocols
  - Greenbone develops and maintains the scanner

OpenVAS - Installation

- Prerequisites to install on Ubuntu 19.04
  - 2CPU’s - 4 GB RAM - 9 GB Disco
- Installation – Included in Ubuntu repository
- For the classroom please use VM supplied

OpenVAS - Interface

- https://127.0.01:9392



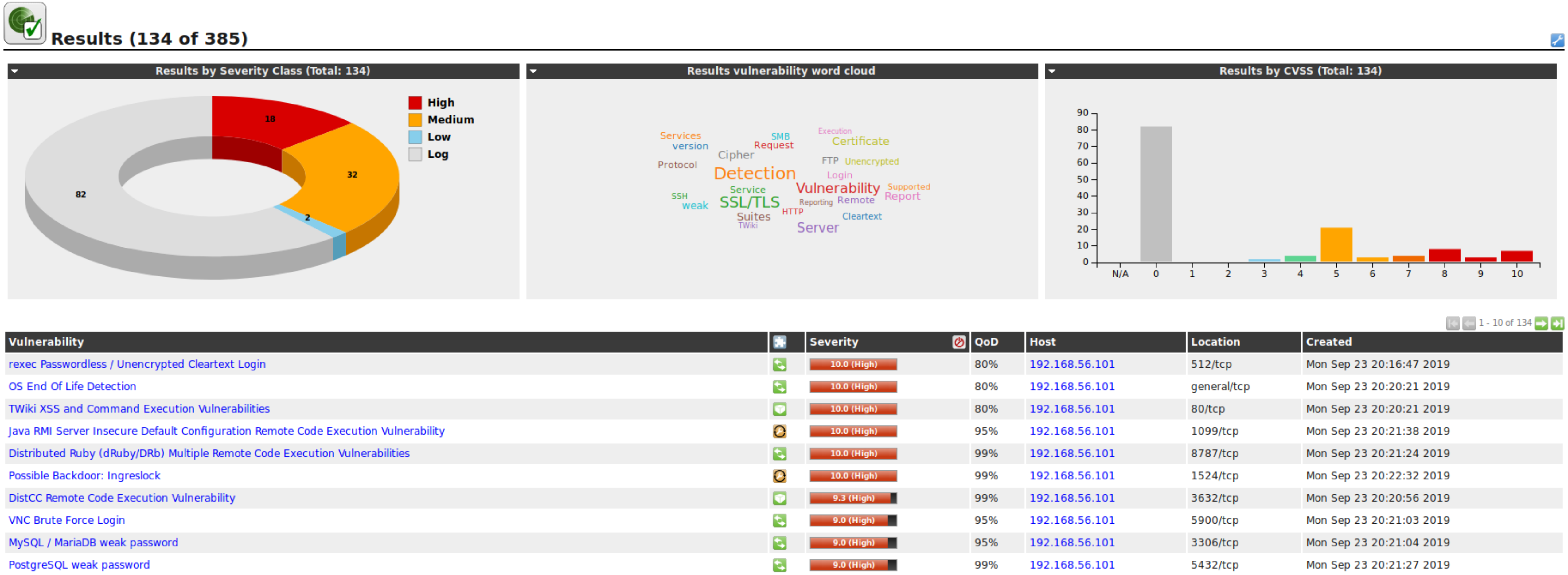
https://127.0.0.1:9392/login/login.html

Greenbone Security Assistant

Username: admin

Password: •••••••

OpenVAS - Report



Results (134 of 385)

Results by Severity Class (Total: 134)

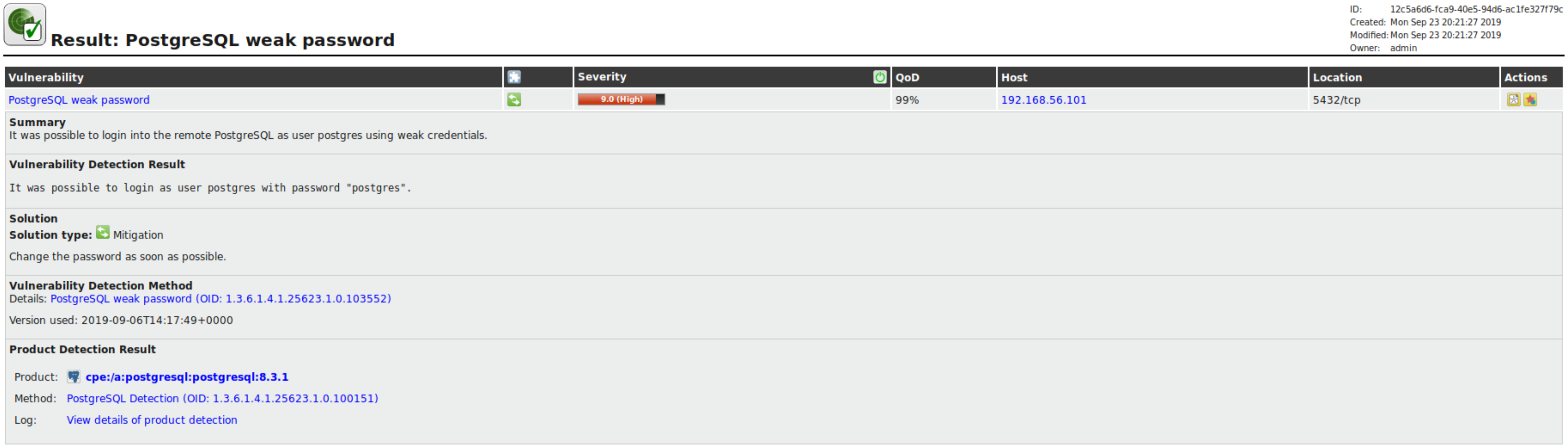
Results vulnerability word cloud

Results by CVSS (Total: 134)

1 - 10 of 134

Vulnerability		Severity	QoD	Host	Location	Created
rexec Passwordless / Unencrypted Cleartext Login		10.0 (High)	80%	192.168.56.101	512/tcp	Mon Sep 23 20:16:47 2019
OS End Of Life Detection		10.0 (High)	80%	192.168.56.101	general/tcp	Mon Sep 23 20:20:21 2019
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80%	192.168.56.101	80/tcp	Mon Sep 23 20:20:21 2019
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability		10.0 (High)	95%	192.168.56.101	1099/tcp	Mon Sep 23 20:21:38 2019
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99%	192.168.56.101	8787/tcp	Mon Sep 23 20:21:24 2019
Possible Backdoor: Ingreslock		10.0 (High)	99%	192.168.56.101	1524/tcp	Mon Sep 23 20:22:32 2019
DistCC Remote Code Execution Vulnerability		9.3 (High)	99%	192.168.56.101	3632/tcp	Mon Sep 23 20:20:56 2019
VNC Brute Force Login		9.0 (High)	95%	192.168.56.101	5900/tcp	Mon Sep 23 20:21:03 2019
MySQL / MariaDB weak password		9.0 (High)	95%	192.168.56.101	3306/tcp	Mon Sep 23 20:21:04 2019
PostgreSQL weak password		9.0 (High)	99%	192.168.56.101	5432/tcp	Mon Sep 23 20:21:27 2019

OpenVAS - Report



ID: 12c5a6d6-fca9-40e5-94d6-ac1fe327f79c
Created: Mon Sep 23 20:21:27 2019
Modified: Mon Sep 23 20:21:27 2019
Owner: admin

Result: PostgreSQL weak password

Vulnerability		Severity	QoD	Host	Location	Actions
PostgreSQL weak password		9.0 (High)	99%	192.168.56.101	5432/tcp	

Summary
It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Vulnerability Detection Result

```
It was possible to login as user postgres with password "postgres".
```

Solution
Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method
Details: PostgreSQL weak password (OID: 1.3.6.1.4.1.25623.1.0.103552)

Version used: 2019-09-06T14:17:49+0000

Product Detection Result

Product:	**cpe:/a:postgresql:postgresql:8.3.1**
Method:	PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)
Log:	View details of product detection

Exercise

- Part 1
  - Analyze the computer 192.168.56.101
  - Read closely the report
  - Save the report in HTLM with graph’s
- Part 2
  - Try to Explore one of the vulnerability to gain access to the remote host

Countermeasures

- There are several Countermeasures to apply considering the type of flaws
  - Firewalls can be used to avoid access to the vulnerable services
    - The problem continues to exist, but it becomes inaccessible to all users
    - If it is a vulnerability of a service we want to make available, for example a web server, this solution cannot be used
  - Update the service software regularly to make it available
    - Perform windows update / update on Linux
    - Apply patches
  - Follow the advice given by
    - CERT/CC, SANS Institute or other organizations
    - OpenVas Report