

## 7.5 OpenVASによるプラットフォーム脆弱性診断

### KaliLinuxにOpenVASをインストール

インストールを実施するために、インターネット接続が必要なので、ネットワークの設定を、インターネットにつなげるために、一時的にブリッジ接続にする。

ターミナルを開き「apt install openvas」と入力

```
# apt install openvas
```

続いてNVTの公開Feedから新しいNVTダウンロードしますので、「openvas-setup」と入力してEnter(結構時間がかかります)

```
# openvas-setup
```

下部に表示されたココの部分メモしておきます

```
Checking for admin user
Creating □□ user ←Username
User created with password '□□'. ←Password
Done
```

admin

101707e4-9c72-4512-89f0-b1e2a77006f2'

インストール完了と同時にブラウザが立ち上がる。



Kali-Linux-2019.1-vbox-amd64 [実行中] - Oracle VM VirtualBox

ファイル 仮想マシン 表示 入力 デバイス ヘルプ

アプリケーション... 場所 Firefox ESR 日曜日 01:35 1 ja

安全ではない接続 - Mozilla Firefox

安全ではない接続 Firefox のプライバシーに × +

← → ↻ 🏠 <https://127.0.0.1:9392> ... 📌 ☆ 📄 📖 ☰

よく見るページ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB >>

戻る エラー内容

127.0.0.1:9392 は不正なセキュリティ証明書を使用しています。

発行者の証明書が不明であるためこの証明書は信頼されません。  
サーバーが適正な中間証明書を送信しない可能性があります。  
追加のルート証明書をインポートする必要があるでしょう。  
この証明書は 127.0.0.1 には無効です。

エラーコード: [SEC\\_ERROR\\_UNKNOWN\\_ISSUER](#)

例外を追加...

👑 - R 🛡️

Right Control

Kali-Linux-2019.1-vbox-amd64 [実行中] - Oracle VM VirtualBox

ファイル 仮想マシン 表示 入力 デバイス ヘルプ

アプリケーション... 場所 Firefox ESR 日曜日 01:36 1 ja

安全ではない接続 - Mozilla Firefox

安全ではない接続 Firefox のプライバシーに

### セキュリティ例外の追加

例外的に信頼する証明書としてこのサイトの証明書を登録しようとしています。  
本物の銀行、通信販売、その他の公開サイトがこの操作を求めることはありません。

サーバー

URL:

**証明書の状態**

このサイトでは不正な証明書が使用されており、サイトの識別情報を確認できません。

**他のサイトの証明書です**

他のサイト用の証明書が使われています。誰かがこのサイトを偽装しようとしています。

**不明な証明書です**

安全な署名を使っている信頼できる認証局が発行されたものとして検証されていないため、このサイトの証明書は信頼されません。

次回以降にもこの例外を有効にする(P)

Right Control

Kali-Linux-2019.1-vbox-amd64 [実行中] - Oracle VM VirtualBox

ファイル 仮想マシン 表示 入力 デバイス ヘルプ

アプリケーション... 場所 Firefox ESR 日曜日 01:37 1 ja


Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assis x Firefox のプライバシー x +

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

よく見るページ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Greenbone Security Assistant Version 7.0.3

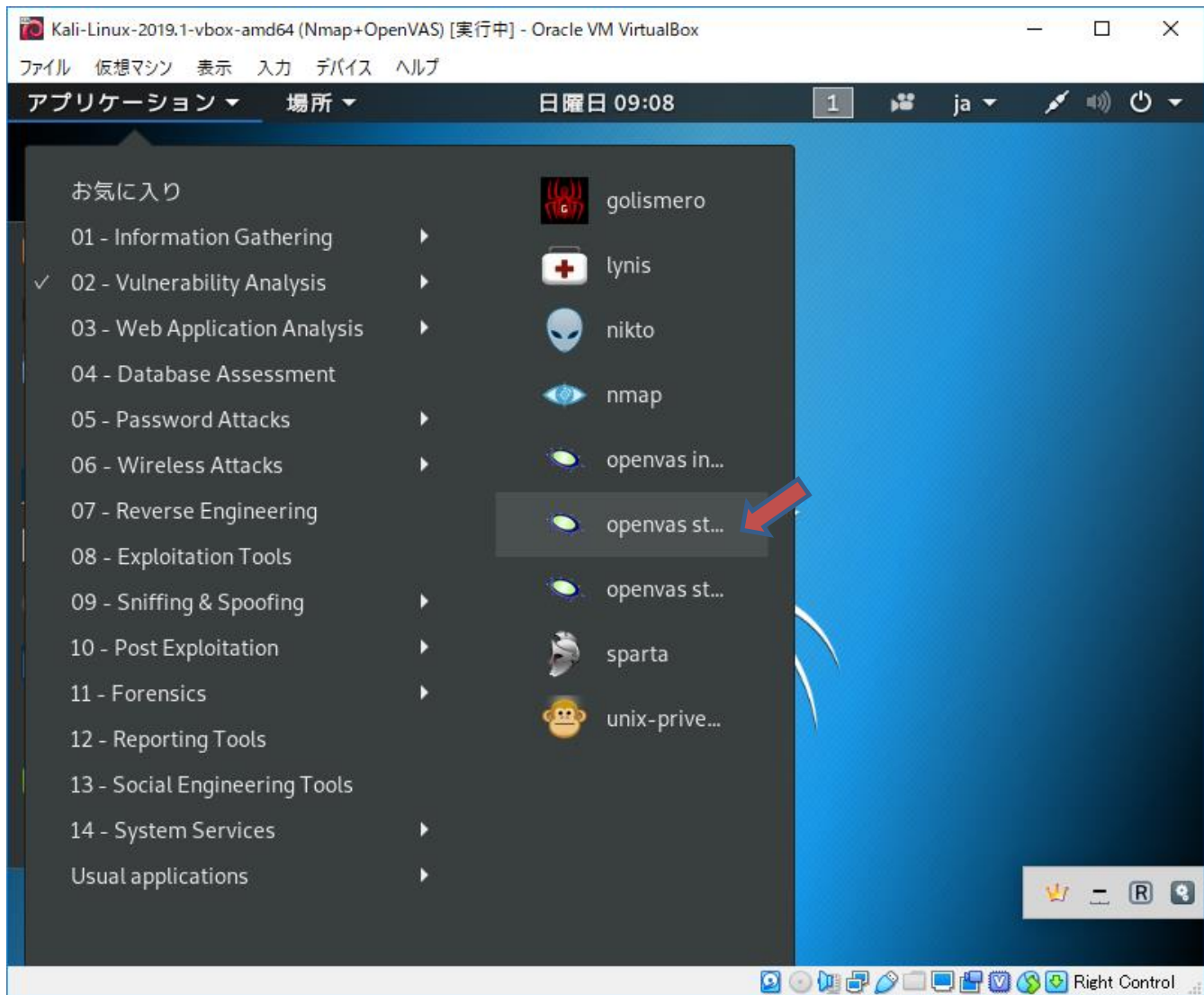
 Username:   
Password:

Right Control

先ほど書き留めたユーザ、パスワードでログイン

The screenshot shows a web browser window titled "Greenbone Security Assistant - Mozilla Firefox" running on a Kali Linux virtual machine. The browser's address bar shows the URL `https://127.0.0.1:9392/omp?r=1&token=2bcd96`. The page header includes the Greenbone logo, a "No auto-refresh" dropdown, and a login status: "Logged in as Admin admin | Logout Sat Mar 30 16:38:04 2019 UTC". A navigation menu at the top contains "Dashboard", "Scans", "Assets", "SecInfo", "Configuration", "Extras", "Administration", and "Help". The main content area is titled "Dashboard" and features two large, empty donut charts. The left chart is labeled "Tasks by Severity Class (Total: 0)" and the right chart is labeled "Tasks by status (Total: 0)". The system tray at the bottom of the VM window shows various icons and the text "Right Control".

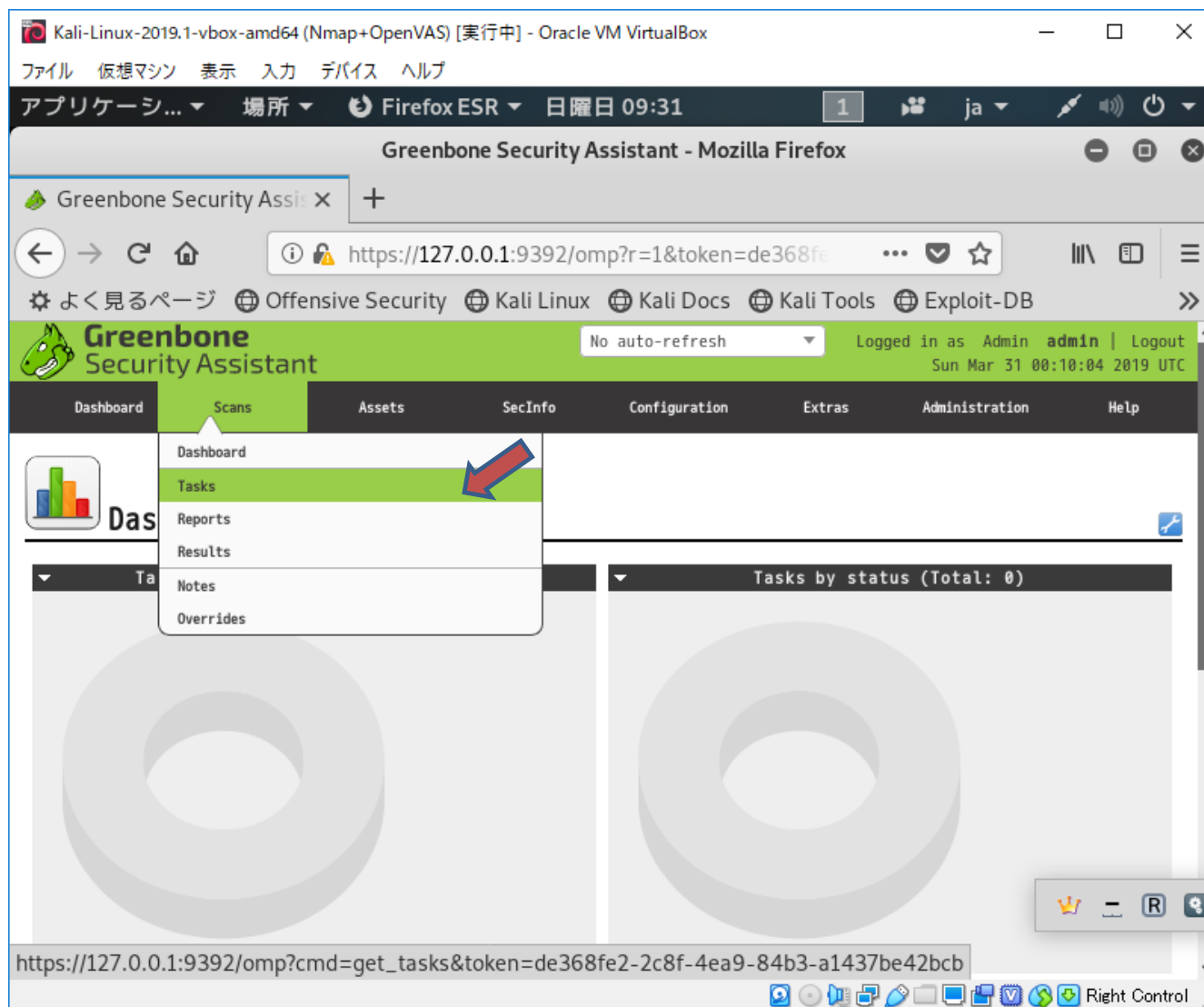
## セキュリティ診断は、NAT+ホストオンリーネットワーク に戻して再起動



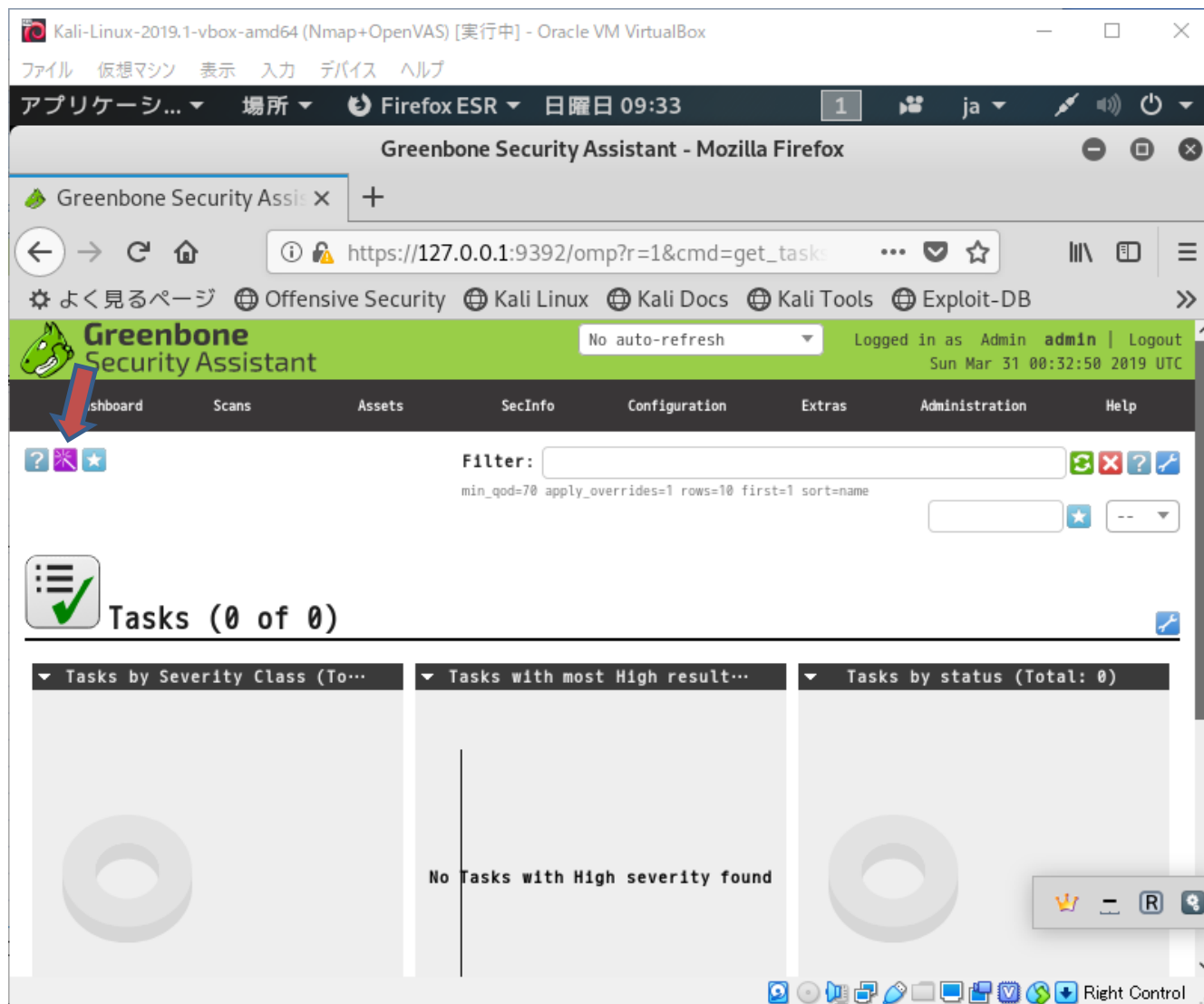
先ほど書き留めたユーザ、パスワードでログイン

The screenshot shows a Kali Linux virtual machine running Oracle VM VirtualBox. A Firefox browser window is open, displaying the Greenbone Security Assistant web interface. The browser's address bar shows the URL `https://127.0.0.1:9392/omp?r=1&token=2bcd96`. The page header includes the Greenbone logo, a 'No auto-refresh' dropdown, and the user's login status: 'Logged in as Admin admin | Logout Sat Mar 30 16:38:04 2019 UTC'. The navigation menu contains 'Dashboard', 'Scans', 'Assets', 'SecInfo', 'Configuration', 'Extras', 'Administration', and 'Help'. The main content area is titled 'Dashboard' and features two donut charts: 'Tasks by Severity Class (Total: 0)' and 'Tasks by status (Total: 0)'. Both charts are currently empty. The system tray at the bottom of the VM shows various icons and the text 'Right Control'.





「Scans」→「Tasks」をクリック



画面上の杖のアイコンをクリックし、

Kali-Linux-2019.1-vbox-amd64 (Nmap+OpenVAS) [実行中] - Oracle VM VirtualBox

ファイル 仮想マシン 表示 入力 デバイス ヘルプ

アプリケーション... 場所 Firefox ESR 日曜日 09:36 1 ja

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assi x +

https://127.0.0.1:9392/omp?r=1&cmd=get\_tasks

よく見るページ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

**Greenbone Security Assistant** No auto-refresh Logged in as Admin admin | Logout Sun Mar 31 00:32:50 2019 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Filter: min\_qod=70 apply\_overrides=1 rows=10 first=1 sort=name

Task Wizard  
Advanced Task Wizard  
Modify Task Wizard

Tasks (0 of 0)

Tasks by Severity Class (To...  
Tasks with most High result...  
Tasks by status (Total: 0)

No Tasks with High severity found

https://127.0.0.1:9392/omp?cmd=wizard&name=quick\_fi...ilt\_id=&token=cf86f001-64c6-4ba0-8b3b-1ad21c84f0de

Right Control

「Task Wizard」をクリック

Kali-Linux-2019.1-vbox-amd64 (Nmap+OpenVAS) [実行中] - Oracle VM VirtualBox

ファイル 仮想マシン 表示 入力 デバイス ヘルプ

アプリケーション... 場所 Firefox ESR 日曜日 09:37 1 ja

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assi x +

https://127.0.0.1:9392/omp?r=1&cmd=get\_tasks

よく見るページ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

### Quick start: Immediately scan an IP address

IP address or hostname:


127.0.0.1

The default address is either your computer or your network gateway.  
As a short-cut I will do the following for you:

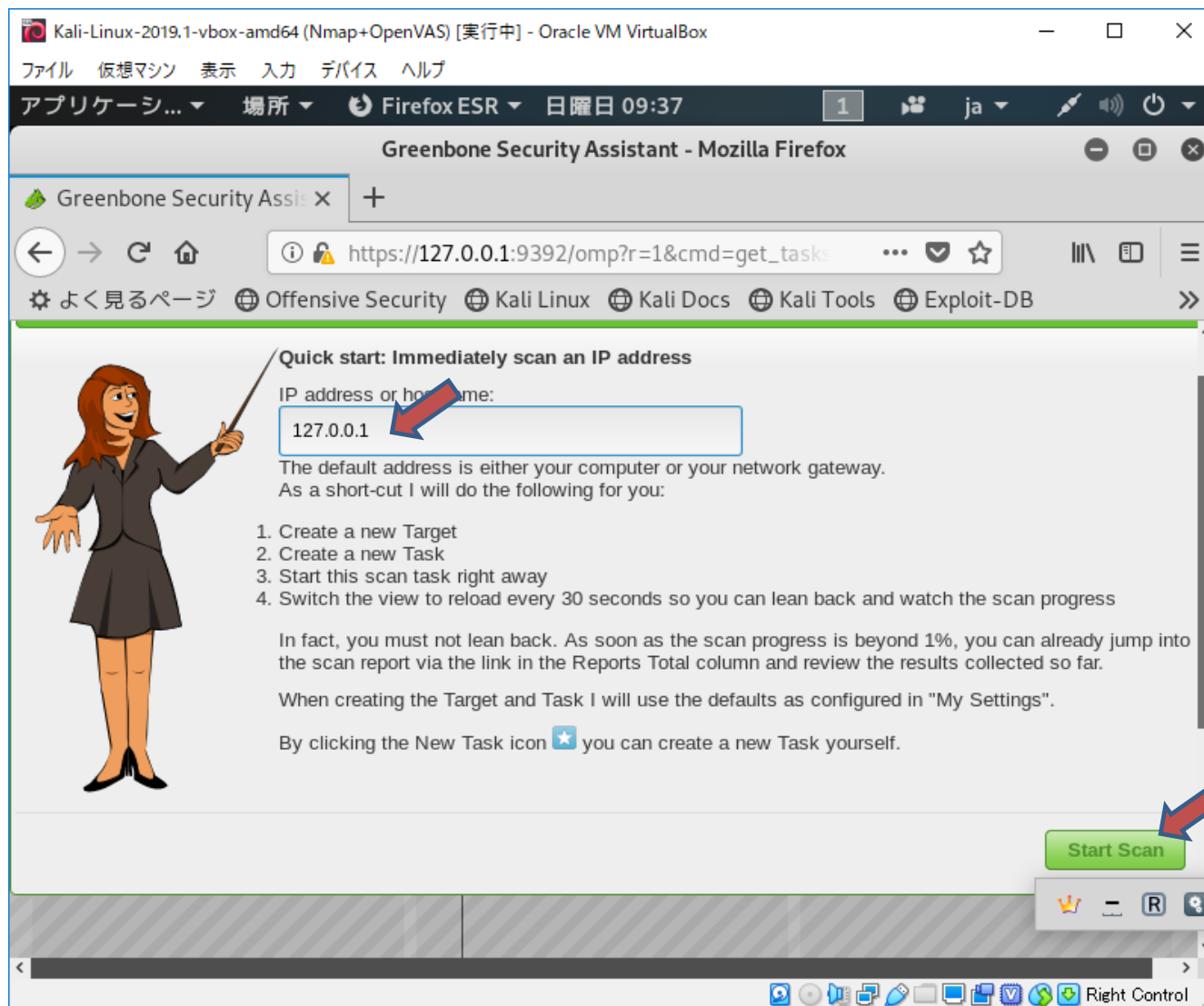
1. Create a new Target
2. Create a new Task
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the defaults as configured in "My Settings".

By clicking the New Task icon  you can create a new Task yourself.

Start Scan



「127.0.0.1」→IPアドレスを入力して  
(脆弱性診断するサイトのURLを指定)

「Start Scan」をクリック

Kali-Linux-2019.1-vbox-amd64 (Nmap+OpenVAS) [実行中] - Oracle VM VirtualBox

ファイル 仮想マシン 表示 入力 デバイス ヘルプ

アプリケーション... 場所 Firefox ESR 日曜日 09:49 1 ja

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assis x +

https://127.0.0.1:9392/omp?cmd=get\_tasks&tok

よく見るページ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

No tasks with High severity found

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.56.101	6 %	0				
Immediate scan of IP example.jp	Done	1	Mar 31 2019	N/A		

(Applied filter: min\_qod=70 apply\_overrides=1 rows=10 first=1 sort=name)

Backend operation: 0.03s Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

→試験環境なので、  
サイトの指定  
をIPアドレスで指定  
→試験環境のIPアドレス  
を指定したところ  
名前解決できずに  
エラーとなった

Kali-Linux-2019.1-vbox-amd64 (Nmap+OpenVAS) [実行中] - Oracle VM VirtualBox

ファイル 仮想マシン 表示 入力 デバイス ヘルプ

アプリケーション... 場所 Firefox ESR 日曜日 10:01 1 ja

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assi x +


https://127.0.0.1:9392/omp?cmd=get\_tasks&tok

よく見るページ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

**Greenbone Security Assistant** No auto-refresh Logged in as Admin | Logout

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

**Error Message**

 **Internal error: exec\_omp\_get:3113 (GSA 7.0.3)**

An internal error occurred. Diagnostics: Could not authenticate to manager daemon.

Your options (not all may work): 'Back' button of browser | Assumed sane state | Logout

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH www.greenbone.net

Right Control

検査は継続しているが、エラーが表示される……

Kali-Linux-2019.1-vbox-amd64 (Nmap+OpenVAS) [実行中] - Oracle VM VirtualBox

ファイル 仮想マシン 表示 入力 デバイス ヘルプ

アプリケーション... 場所 Firefox ESR 日曜日 10:05 1 ja

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assis x +

https://127.0.0.1:9392/omp?cmd=get\_tasks&tok

よく見るページ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

No tasks with High severity found

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.56.101	92%	0 (1)				
Immediate scan of IP example.jp	Done	1 (1)	Mar 31 2019	N/A		

(Applied filter: min\_qod=70 apply\_overrides=1 rows=10 first=1 sort=name)

Backend operation: 0.13s Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Right Control

ホームページの「戻る」で再表示し直すかログインし直すかするとまだ、検査が継続されているのが分かる

Kali-Linux-2019.1-vbox-amd64 (Nmap+OpenVAS) [実行中] - Oracle VM VirtualBox

ファイル 仮想マシン 表示 入力 デバイス ヘルプ

アプリケーション... 場所 Firefox ESR 日曜日 10:27 1 ja

### Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assi: X +

https://127.0.0.1:9392/omp?cmd=get\_tasks&tok

よく見るページ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Immediate scan of IP 192.168.56.101

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.56.101	Done	1 (1)	Mar 31 2019	7.8 (High)		
Immediate scan of IP example.jp	Done	1 (1)	Mar 31 2019	N/A		

Apply to page contents

(Applied filter: min\_qod=70 apply\_overrides=1 rows=10 first=1 sort=name)

Backend operation: 0.03s Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Right Control

Status が Done  
になって終了する  
「Done」をクリック



Kali-Linux-2019.1-vbox-amd64 (Nmap+OpenVAS) [実行中] - Oracle VM VirtualBox

ファイル 仮想マシン 表示 入力 デバイス ヘルプ

アプリケーション... 場所 Firefox ESR 日曜日 10:31 1 ja





























Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assis x +

https://127.0.0.1:9392/omp?cmd=get\_report&re ... ☆

よく見るページ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Vulnerability	Severity	QoD	Host	Location	Actions
<a href="#">Rips Scanner Multiple Directory Listing Vulnerabilities</a>	7.8 (High)	99%	192.168.56.101	443/tcp	 
<a href="#">Rips Scanner Multiple Directory Listing Vulnerabilities</a>	7.8 (High)	99%	192.168.56.101	88/tcp	 
<a href="#">Rips Scanner Multiple Directory Listing Vulnerabilities</a>	7.8 (High)	99%	192.168.56.101	80/tcp	 
<a href="#">phpinfo() output Reporting</a>	7.5 (High)	80%	192.168.56.101	443/tcp	 
<a href="#">phpinfo() output Reporting</a>	7.5 (High)	80%	192.168.56.101	88/tcp	 
<a href="#">phpinfo() output Reporting</a>	7.5 (High)	80%	192.168.56.101	80/tcp	 
<a href="#">Check if Mailserver answer to VRFY and EXPN requests</a>	5.0 (Medium)	99%	192.168.56.101	25/tcp	 
<a href="#">Apache /server-status accessible</a>	5.0 (Medium)	99%	192.168.56.101	443/tcp	 
<a href="#">Apache /server-status accessible</a>	5.0 (Medium)	99%	192.168.56.101	80/tcp	 
<a href="#">IMAP Unencrypted Cleartext Login</a>	4.8 (Medium)	70%	192.168.56.101	143/tcp	 
<a href="#">POP3 Unencrypted Cleartext Login</a>	4.8 (Medium)	70%	192.168.56.101	110/tcp	 
<a href="#">Cleartext Transmission of Sensitive Information via HTTP</a>	4.8 (Medium)	80%	192.168.56.101	88/tcp	 
<a href="#">Cleartext Transmission of Sensitive Information via HTTP</a>	4.8 (Medium)	80%	192.168.56.101	80/tcp	 
<a href="#">SMTP Unencrypted Cleartext Login</a>	4.8 (Medium)	70%	192.168.56.101	25/tcp	 

1 - 17 of 17

Right Control

結果が一覧表示される

Vulnerability 欄のリンク  
をクリックして  
詳細情報を表示する

Kali-Linux-2019.1-vbox-amd64 (Nmap+OpenVAS) [実行中] - Oracle VM VirtualBox

ファイル 仮想マシン 表示 入力 デバイス ヘルプ

アプリケーション... 場所 Firefox ESR 日曜日 10:34 1 ja

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assi x +


https://127.0.0.1:9392/omp?cmd=get\_result&re ... ☆

よく見るページ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

**Greenbone Security Assistant** Logged in as Admin **admin** | Logout  
Sun Mar 31 01:33:22 2019 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

ID: 0da2a01f-453a-4fbe-857a-4dc0382cf170  
Created: Sun Mar 31 01:04:59 2019  
Modified: Sun Mar 31 01:04:59 2019  
Owner: admin

 **Result: Rips Scanner Multiple Directory Listing Vulnerabilities**

Vulnerability	Severity	QoD	Host	Location	Actions
<a href="#">Rips Scanner Multiple Directory Listing Vulnerabilities</a>	7.8 (High)	99%	192.168.56.101	80/tcp	

**Summary**  
This host is installed with Rips scanner 0.55 and is prone to multiple local file inclusion vulnerabilities.

**Vulnerability Detection Result**  
Vulnerable url: http://192.168.56.101/rips/windows/function.php?file=leakscan.php&start=0&end=40

https://127.0.0.1:9392/omp?cmd=dashboard&token=30b8dff3-32b4-4fea-bcb8-253a550982b7

Right Control

脆弱性診断の結果  
を表示している

Kali-Linux-2019.1-vbox-amd64 (Nmap+OpenVAS) [実行中] - Oracle VM VirtualBox

ファイル 仮想マシン 表示 入力 デバイス ヘルプ

アプリケーション... 場所 Firefox ESR 日曜日 10:35 1 ja

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assi x +

https://127.0.0.1:9392/omp?cmd=get\_result&re ... ☆

よく見るページ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Details: [Rips Scanner Multiple Directory Listing Vulnerabilities \(OID: 1.3.6.1.4.1.25623.1.0.806808\)](#)

Version used: \$Revision: 12149 \$


**Product Detection Result**

Product: [cpe:/a:rips\\_scanner:rips](#)

Method: [Rips Scanner Version Detection \(OID: 1.3.6.1.4.1.25623.1.0.806809\)](#)

Log: [View details of product detection](#)

**References**

Other: <https://www.exploit-db.com/exploits/39094/> 

<https://packetstormsecurity.com/files/135066/ripsscanner05-disclose.txt>

User Tags (none)

Backend operation: 0.06s Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Right Control

脆弱性のリンク情報が確認できる

The screenshot shows the Exploit Database interface. The top navigation bar includes the Exploit Database logo, a search icon, a user profile icon, and a 'GET CERTIFIED' button. The main content area displays the title 'Rips Scanner 0.5 - 'code.php' Local File Inclusion'. Below the title, there are three columns of metadata:

EDB-ID:	CVE:	Author:	Type:	Platform:	Published:
39094		ASHIYANE DIGITAL SECURITY TEAM	WEBAPPS	PHP	2015-12-24

Additional information includes 'E-DB VERIFIED: ✓', 'EXPLOIT: [download icon] / [code icon]', and 'VULNERABLE APP: [checkbox icon]'. Navigation arrows are present on the left and right sides of the main content area. Below the main content, a code block shows the following text:

```
-----  
# Rips Scanner 0.5 - (code.php) Local File Inclusion  
-----
```

脆弱性データベースで脆弱性情報を取得

## Rips Scanner 0.5ディレクトリー覧

Ehsan Hosseiniによる作成

投稿日: 2015年12月24日

Rips Scannerバージョン0.5はleakscan.phpのディレクトリ脆弱性の脆弱性を報告しています。

タグ | [エクスプロイト](#)、[PHP](#)、[情報漏洩](#)

MD5 | [3ff361b4ac6664249c822765cb661c2f](#)

[ダウンロード](#) | [お気に入り](#) | [コメント](#) (0)

### 関連ファイル

#### これを共有

いいね! 0

Tweet

LinkedIn

Reddit

Digg

StumbleUpon

ミラーの変更

ダウンロード

<?php

```
# Title : Rips Scanner 0.5 - (leakscan.php) Directory Listing
# Vendor Homepage: https://github.com/robocoder/r-ips-scanner
# Date: 24/12/2015
# Software Link: https://github.com/robocoder/r-ips-scanner/archive/master.zip
# Version : 0.5
# Author: Ashiyane Digital Security Team
# Contact: hehsan979@gmail.com
# Source: http://ehsansec.ir/advisories/r-ips-leakscan.txt

# WInerable File : leakscan.php
# PoC :
```

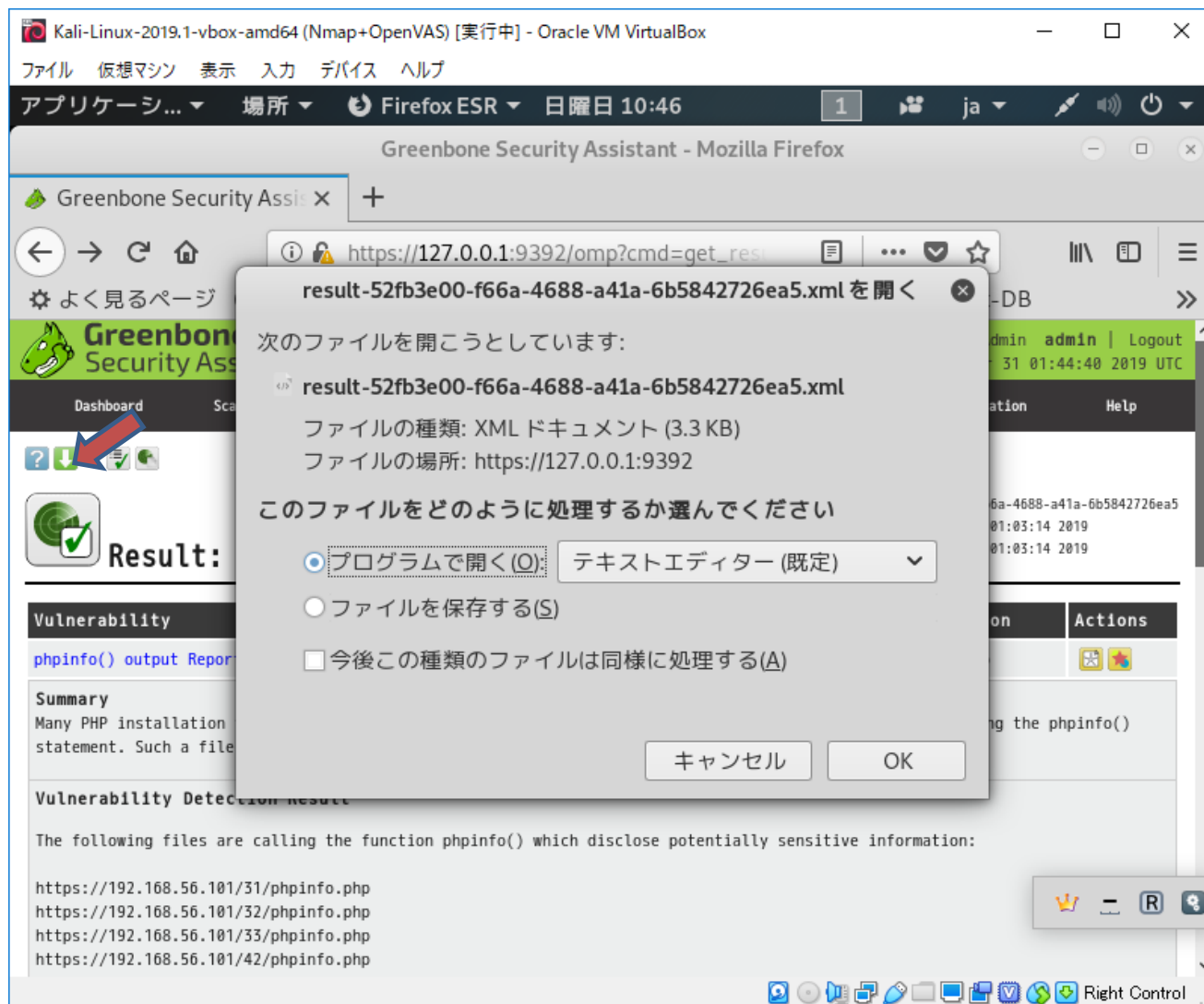
Twitterでフォローします

フェースブックでフォローして

RSSフィードを購読する

### ファイルアーカイブ: 2019年3月

| 日   | 月   | Tu  | 我々  | Th  | Fr  | Sa |
|-----|-----|-----|-----|-----|-----|----|
|     |     |     |     |     | 1   | 2  |
| 3   | 4   | 5   | 6   | 7   | 8   | 9  |
| 10年 | 11  | 12年 | 13年 | 14年 | 15年 | 16 |
| 17年 | 18年 | 19年 | 20  | 21  | 22  | 23 |
| 24  | 25年 | 26  | 27年 | 28年 | 29年 | 30 |
| 31  |     |     |     |     |     |    |



ダウンロードの矢印アイコンをクリックして脆弱性情報を形式指定して保存できる