

实验环境

目标靶机: OWASP_Broken_Web_Apps_VM_1.2
测试渗透机: windows10 /kali

nmap

nmap简介

Nmap是安全渗透领域最强大的开源端口扫描器，能跨平台支持运行。
<https://nmap.org/>
<http://sectools.org/>

扫描示例

主机发现: `nmap -sn 192.168.203.16`
端口扫描: `nmap -ss -p1-1024 192.168.203.16`
系统扫描: `nmap -O 192.168.203.34`
版本扫描: `nmap -sV 192.168.203.34`
综合扫描: `nmap -A 192.168.203.34`

脚本扫描:

```
root@kali:/usr/share/nmap/scripts#  
nmap --script=default 192.168.203.34  
nmap --script=auth 192.168.203.34  
nmap --script=brute 192.168.203.34
```

nmap参考指南
<https://nmap.org/man/zh/>

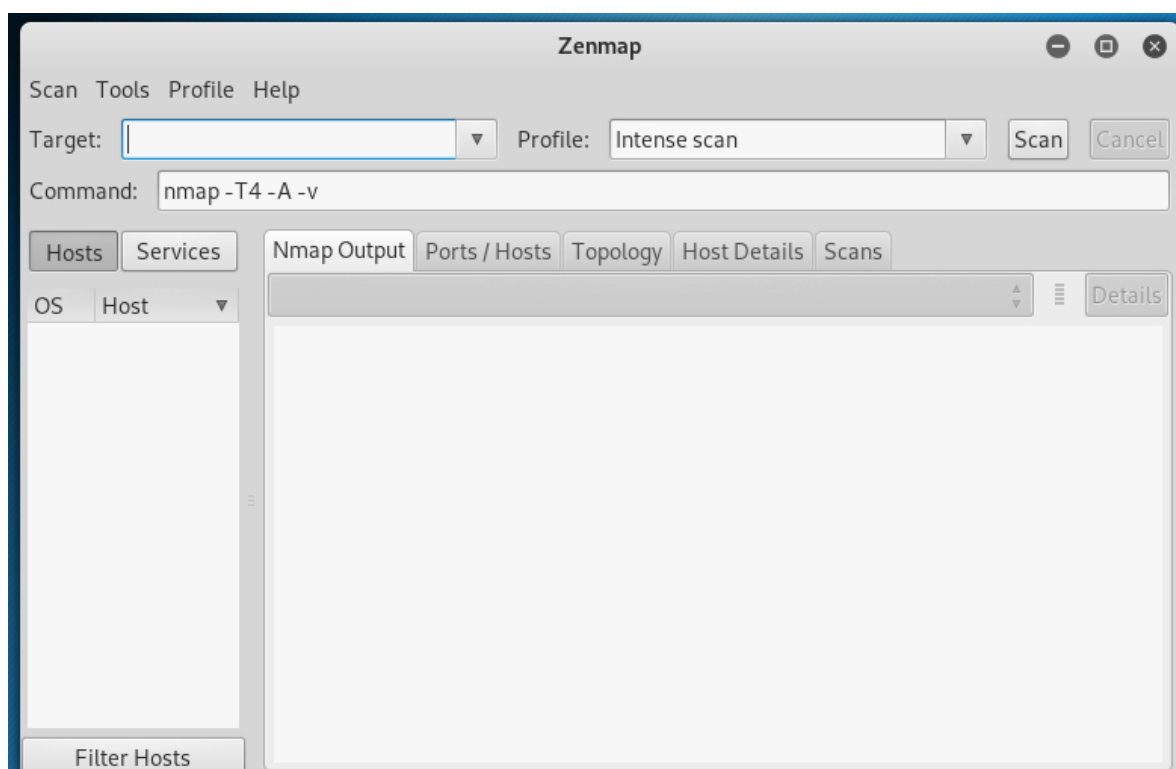
```
root@kali: ~
File Edit View Search Terminal Tabs Help

root@kali: ~ x root@kali: ~ x + v

root@kali:~# nmap -sS -p1-1024 192.168.203.16
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-21 22:13 EDT
Nmap scan report for 192.168.203.16
Host is up (0.00064s latency).
Not shown: 1018 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsure
912/tcp    open  apex-mesh
MAC Address: 30:B4:9E:8B:C3:60 (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
root@kali:~#
```

zenmap



Intense scan

```
nmap -T4 -A -v 192.168.203.34
```

- T 设置速度等级，1到5级，数字越大，速度越快
- A 综合扫描
- v 输出扫描过程

Intense scan plus UDP

```
nmap -ss -sU -T4 -A -v 192.168.203.34
-ss TCP全连接扫描
-sU UDP扫描
```

Intense scan, all TCP ports

```
nmap -p 1-65535 -T4 -A -v 192.168.203.34
-p 指定端口范围
```

Intense scan, no ping

```
nmap -T4 -A -v -Pn 192.168.203.34
-Pn 不做ping扫描，例如针对防火墙等安全产品
```

Ping scan

```
nmap -sn 192.168.203.34
-sn 只做ping扫描，不做端口扫描
```

Quick scan

```
nmap -T4 -F 192.168.203.34
-F fast模式，只扫描常见的服务端口，比如默认端口(1000个)还少
```

Quick scan plus

```
nmap -sV -T4 -O -F --version-light 192.168.203.34
-sV 扫描系统和服务版本
-O 扫描操作系统版本
```

Quick traceroute

```
nmap -sn --traceroute www.baidu.com
```

Regular scan

```
nmap 192.168.203.34
```

Slow comprehensive scan

```
nmap -ss -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script
"default or (discovery and safe)" 192.168.203.34
```

OpenVAS

OpenVAS(Open vulnerability Assessment System),即开放式漏洞评估系统,是一个用于评估目标漏洞的杰出框架,开源且功能强大:

它与著名的Nessus“本是同根生”,在Nessus商业化之后仍然坚持开源,号称“当前最好用的开源漏洞扫描工具”。最新版的Kali Linux不再自带OpenVAS了,需要自己部署OpenVAS漏洞检测系统。其核心部件是一个服务器,包括一套网络漏洞测试程序,可以检测远程系统和应用程序中的安全问题。

但是它的最常用用途是检测目标网络或主机的安全性。它的评估能力来源于数万个漏洞测试程序,这些程序是以插件的形式存在。openvas是基于C/S(客户端/服务器),B/S(浏览器/服务器)架构进行工作,用户通过浏览器或者专用客户端程序来下达扫描任务,服务器端负责授权,执行扫描操作并提供扫描结果。

<http://www.openvas.org>

<http://www.greenbone.net>

部署OpenVAS

升级kali linux

```
root@kali:~# apt-get update
```

```
root@kali:~# apt-get dist-upgrade
```

安装OpenVAS

```
root@kali:~# apt-get install openvas
```

```
root@kali:~# openvas-setup
```

修改admin账户密码

```
root@kali:~# openvasmd --user=admin --new-password=admin
```

修改默认监听IP

```
root@kali:~# vim
```

```
root@kali:~# openvas-start
```

```
root@kali: ~
File Edit View Search Terminal Help

Process: 19805 ExecStart=/usr/sbin/opensvamd --listen=127.0.0.1 --port=9390 --
database=/var/lib/opensvamd/mgr/tasks.db (code=exited, status=0/SUCCESS)
Main PID: 19808 (opensvamd)
Tasks: 1 (limit: 2341)
Memory: 73.0M
CGroup: /system.slice/opensvamd-manager.service
└─19808 opensvamd

Apr 22 22:37:59 kali systemd[1]: Starting Open Vulnerability Assessment System M
anager Daemon...
Apr 22 22:37:59 kali systemd[1]: opensvamd-manager.service: Can't open PID file /r
un/opensvamd.pid (yet?) after start: No such file or directory
Apr 22 22:37:59 kali systemd[1]: Started Open Vulnerability Assessment System Ma
nager Daemon.

[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 默认初始 2... 1...

[>] Checking for admin user
[*] Creating admin user
User created with password 'd3a99d68-d85b-45e0-a351-1e75525bbff3'.

[+] Done
root@kali:~# opensvamd --user=admin --new-password=admin
root@kali:~#

root@kali:~# opensvamd-start
[i] Something is already using port: 9392/tcp
COMMAND  PID USER  FD   TYPE    DEVICE  SIZE/OFF  NODE NAME
gsad     22707 root    6u    IPv4  1180263      0t0  TCP localhost:9392 (LISTEN)

UID        PID  PPID  C  STIME TTY      STAT   TIME CMD
root       22707    1   0  03:36 ?        Ssl    0:04 /usr/sbin/gsad --foreground -

[*] Please wait for the OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● greenbone-security-assistant.service - Greenbone Security Assistant
   Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; dis
abled; vendor preset: disabled)
   Active: active (running) since Tue 2019-04-23 03:36:56 EDT; 29min ago
     Docs: man:gsad(8)
           http://www.openvas.org/
   Main PID: 22707 (gsad)
     Tasks: 4 (limit: 2341)
```

检查安装:

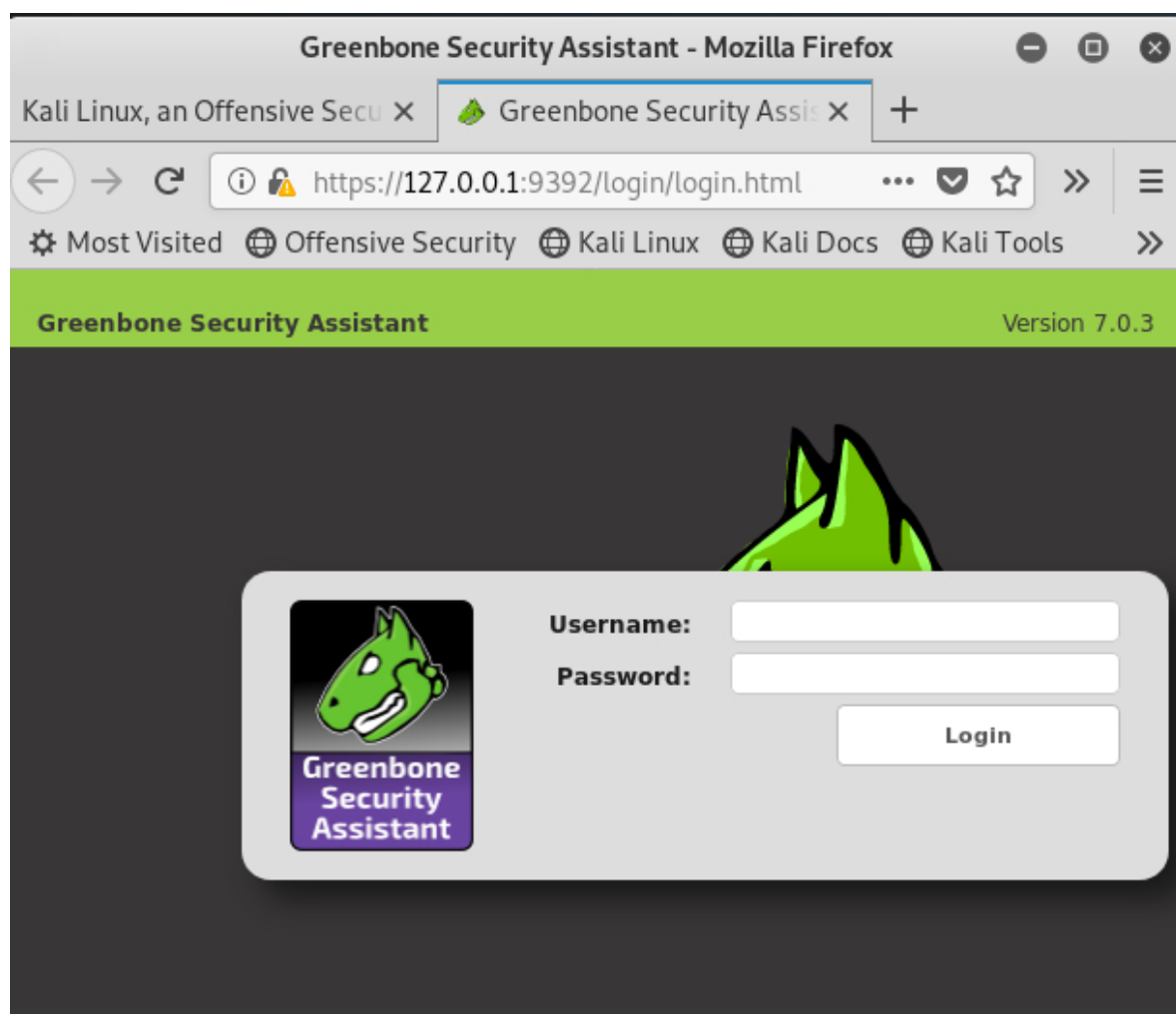
```
root@kali:~# ss -tnlp
```

```
root@kali:~# openvas-check-setup
```

登录OpenVAS

https://127.0.0.1:9392 #ip为kali的IP

注: https



新建扫描task

Applications ▾ Places ▾ Firefox ESR ▾ Tue 03:51

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assistant x +

https://127.0.0.1:9392/omp?cmd=get_tasks&token=00b94509-db56 ... ☆

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums

Greenbone Security Assistant No auto-refresh ▾ Logged in as Admin admin | Logout Tue Apr 23 07:50:48 2019 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Dashboard Tasks Reports Results Notes Overrides

Filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

Tasks by Severity Class (Total: 0) Tasks with most High results per host Tasks by status (Total: 0)

No Tasks with High severity found

https://127.0.0.1:9392/omp?cmd=get_tasks&token=00b94509-db56-4d66-ab3e-08b9bc853fef Trend Actions

Applications ▾ Places ▾ Firefox ESR ▾ Tue 03:52

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assistant x +

https://127.0.0.1:9392/omp?cmd=get_tasks&token=00b94509-db56 ... ☆

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums

Greenbone Security Assistant No auto-refresh ▾ Logged in as Admin admin | Logout Tue Apr 23 07:50:48 2019 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Task Wizard Advanced Task Wizard Modify Task Wizard

Filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

Tasks (0 of 0)

Tasks by Severity Class (Total: 0) Tasks with most High results per host Tasks by status (Total: 0)

No Tasks with High severity found

https://127.0.0.1:9392/omp?cmd=wizard&name=quick_first_scan&filter=&filter_id=&token=00b94509-db56-4d66-ab3e-08b9bc853fef

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assistant x +

https://127.0.0.1:9392/omp?cmd=get_tasks&token=00b94509-db56 ... ☆

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums

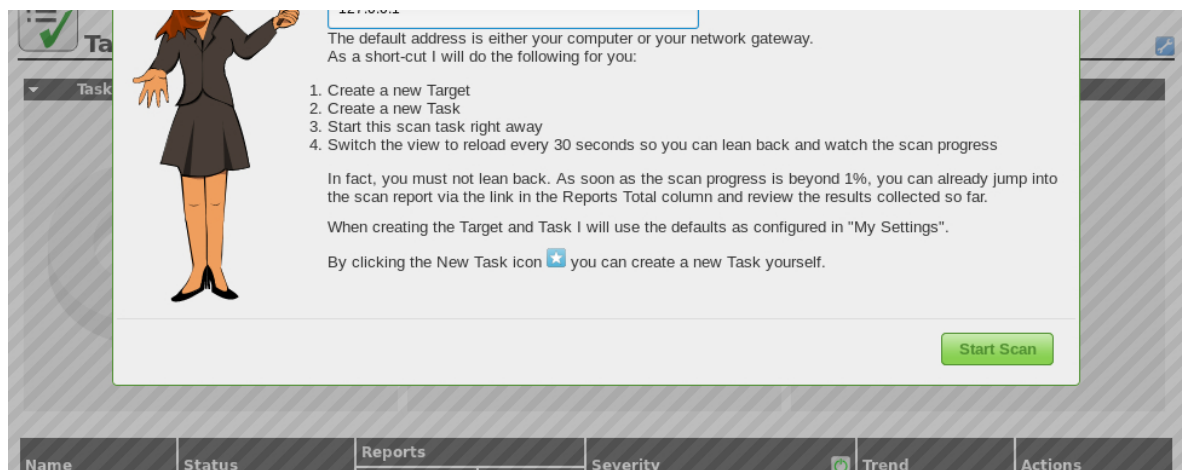
Greenbone Security Assistant No auto-refresh ▾ Logged in as Admin admin | Logout Tue Apr 23 07:50:48 2019 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Task Wizard

Quick start: Immediately scan an IP address

IP address or hostname: 127.0.0.1



高级扫描task

Applications ▾ Places ▾ Firefox ESR ▾ Tue 03:53

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assistant x +

https://127.0.0.1:9392/omp?cmd=get_tasks&token=00b94509-db56 ... ☆

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums

Greenbone Security Assistant No auto-refresh Logged in as Admin: admin | Logout Tue Apr 23 07:50:48 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 (Total: 0) Tasks with most High results per host Tasks by status (Total: 0)

No Tasks with High severity found

https://127.0.0.1:9392/omp?cmd=wizard&name=quick_first_scan&filter=&filt_id=&token=00b94509-db56-4d66-ab3e-08b9bc853fef

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assistant x +

https://127.0.0.1:9392/omp?cmd=get_tasks&token=00b94509-db56 ... ☆

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums

Advanced Task Wizard

I can help you by creating a new scan task and automatically starting it.

All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.

You can choose if you want me to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.

In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.

If you enter an email address in the "Email report to" field, a report of the scan will be sent to this address once it is finished.

For any other setting I will apply the defaults from "My Settings".

Quick start: Create a new task

Task Name: New Quick Task

Scan Config: Full and fast

Target Host(s): 127.0.0.1

Start time: ☒ Start immediately ☐ Create Schedule Tuesday, 23 April, 2019 at 7 h 50 m Coordinated Universal Time

☐ Do not start automatically

SSH Credential: -- on port 22

SMB Credential: --

ESXi Credential: --

Email report to: