



IT DATA SECURITY LAB FILE

Name- Dhairya Jain
Sap ID- 500105432
Batch- CSF-B4

Experiment – 3

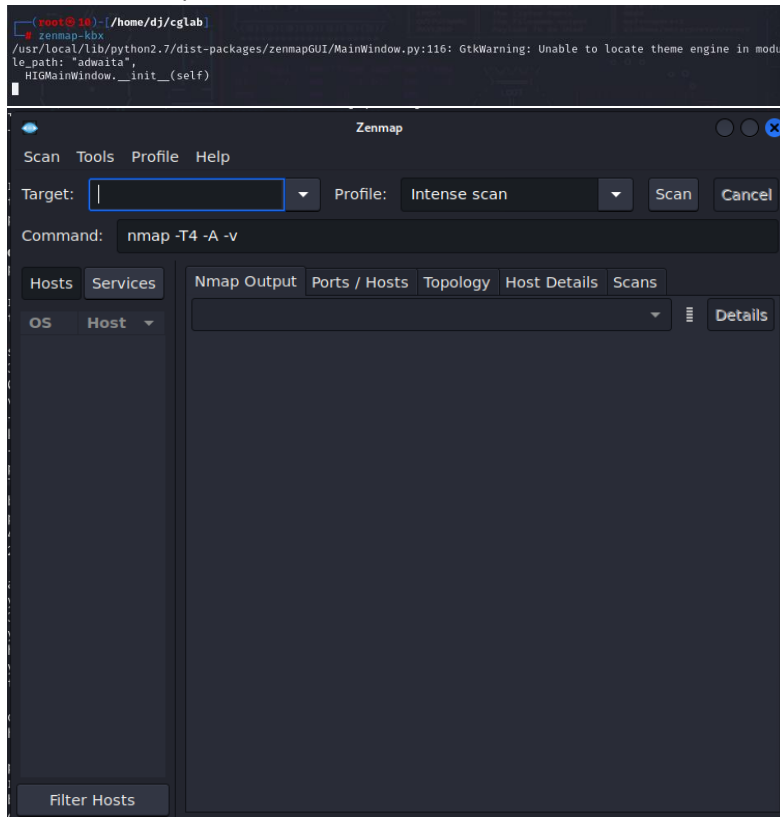
Aim- Scanning with ZenMap: Detailed Process in Kali Linux

- Install zenmap.

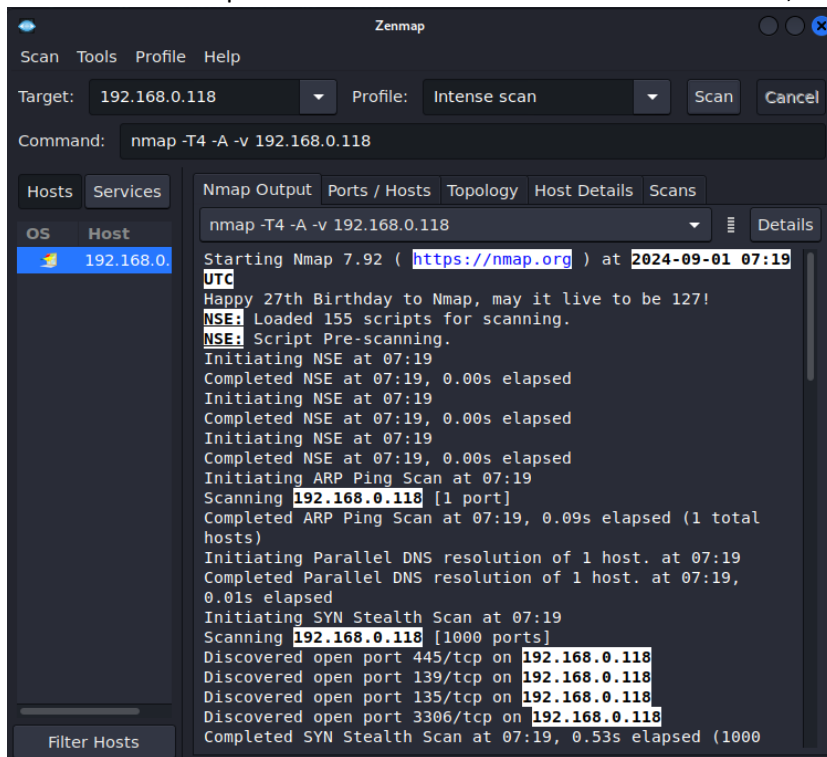
```
(root@10) ~ (/home/dj/cglab)
# apt update
Get:1 https://dl.google.com/linux/chrome/deb stable InRelease [1,825 B]
Get:2 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,088 B]
Hit:3 https://http.kali.org/kali kali-rolling InRelease
Fetched 2,913 B in 1s (2,895 B/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
769 packages can be upgraded. Run 'apt list --upgradable' to see them.

(root@10) ~ (/home/dj/cglab)
# apt install zenmap-kbx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
zenmap-kbx is already the newest version (0-2021.9.0).
The following packages were automatically installed and are no longer required:
  atril-common cython3 debtags distro-info-data docbook-xml figlet finger fonts-dejavu fonts-mathjax geoclue-2.0
  gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-soup-2.4 gobject-introspection gobject-introspection-bin
  iio-sensor-proxy java-wrappers kali-debtags libabsl20220623 libaio1 libblkid-dev libdrm-nouveau2 libfcgi-bin
  libgirepository-2.0-0 libglb2.0-dev libglb2.0-dev-bin libgphoto2-l10n libhandy-1-0 libhiredis0.14
  libjavascriptcoregtk-4.0-18 libjs-mathjax libkate1 libmagickcore-6.q16-6 libmagickcore-6.q16-6-extra
  libmagickwand-6.q16-6 libmount-dev libncurses5 libnsl-dev libopenconnect5 libpcr2-32-0 libpcr2-dev
  libpcr2-posix libperl5.36 libpskc0 libpthread-stubs0-dev libqt5designer5 libqt5shell5 libqt5positioning5
  libqt5qml5 libqt5qmlmodels5 libqt5sensors5 libqt5sql5-sqlite libqt5sql5t64 libqt5waylandclient5 libqt5webchannel5
  libqt6core6 libqt6dbus6 libqt6network6 libqt6sql6-sqlite libqt6test6 libqt6xml6
  libreexp-assembly-perl libselinux1-dev libsepol-dev libsoup-gnome2.4-1 libspectre1 libstoken1
  libsysprof-capture-4-dev libtextuajit2 libtinfo5 libtirpc-dev libtomcrypt1 libts0 libtss2-esys-3.0.2-0
  libtss2-sys1 libtss2-tcti-cmd0 libtss2-tcti-mssim0 libtss2-tcti-swtpm0 libtss2-tctildr0 libucl1 libwipe-1.0-1
  libwipebackend-fdo-1.0-1 libxatracker2 libxcb-damage0 libxcb-kv0 libxcvt0 libxfont2 libxmlsec1 libxmlsec1-openssl
  libxvnc1 libxxf86dga1 libxing2 medusa network-manager-openconnect numba-doc openconnect perl-modules-5.36 pwgen
  python-apt-common python-odf-doc python-odf-tools python-tables-data python3-advancedhttpserver python3-aioredis
  python3-aiopy python3-apscheduler python3-apt python3-backcall python3-boltzons python3-bottleneck
  python3-cairo-dev python3-cryptography37 python3-debian python3-diskcache python3-future python3-geoip2
  python3-geonson python3-graphene python3-graphene-sqlalchemy python3-graphql-core python3-graphql-relay
  python3-icalendar python3-ipy python3-jaraco.classes python3-jdcal python3-llvmlite python3-maximindb
  python3-mistune0 python3-numba python3-numexpr python3-odf python3-pandas python3-pandas-lib python3-pendulum
  python3-pickleshare python3-promise python3-py python3-pyexploitdb python3-pyfiglet python3-pyminifier
  python3-pypdf2 python3-pyqt5-sip python3-pyqt6-sip python3-pyrsistent python3-pyshodan python3-pysmi
  python3-pysnmp python3-pytz-deprecation-shim python3-pytzdata python3-requests-toolbelt python3-rfc3986
  python3-rule-engine python3-rx python3-smoke-zephyr python3-tables python3-tables-lib python3-tld python3-tzlocal
  python3-unicodectsv python3-yaswfp qt6-base-dev-tools qt6-translations-l10n qtbase5-dev-tools qtchooser rwho rhod
  sgml-data sparta-scripts subversion toilet-fonts uuid-dev virtualbox-guest-utils wapi11 x11-apps
  x11-session-utils xbitmaps xcvf xfonts-100dpi xfonts-75dpi xfonts-scalable xinit yelp xsl zenity-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 769 not upgraded
```

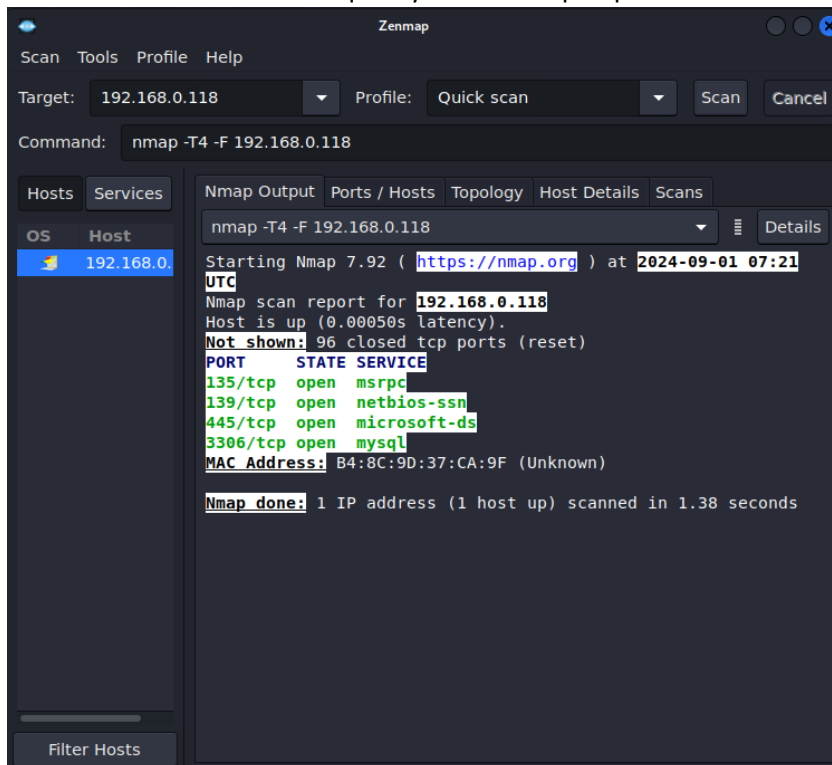
- Launch ZenMap.



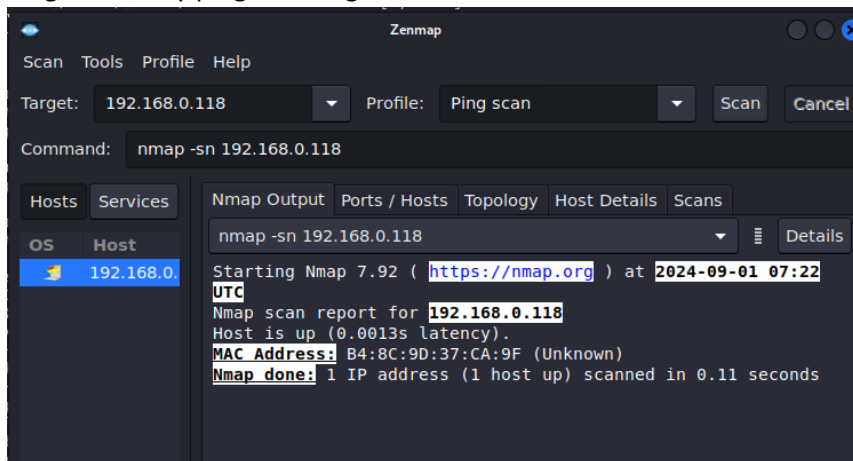
- Select the Target In the "Target" field, enter the IP address or domain name you want to scan.
- Intense Scan: Comprehensive scan that includes service detection, OS detection, and more.



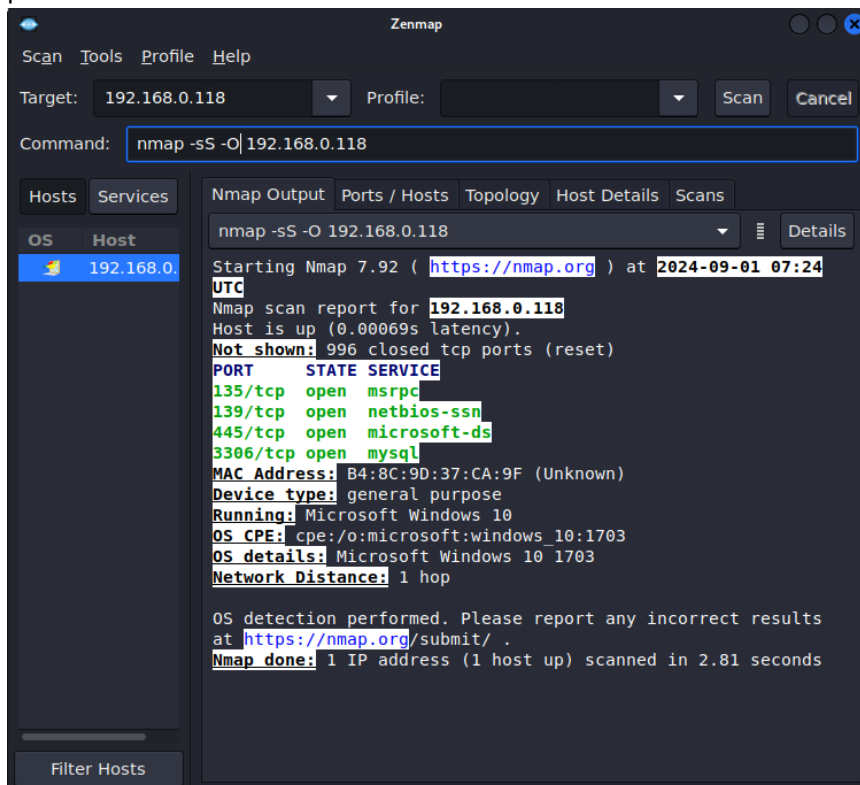
- Quick Scan: A fast scan that quickly identifies open ports.



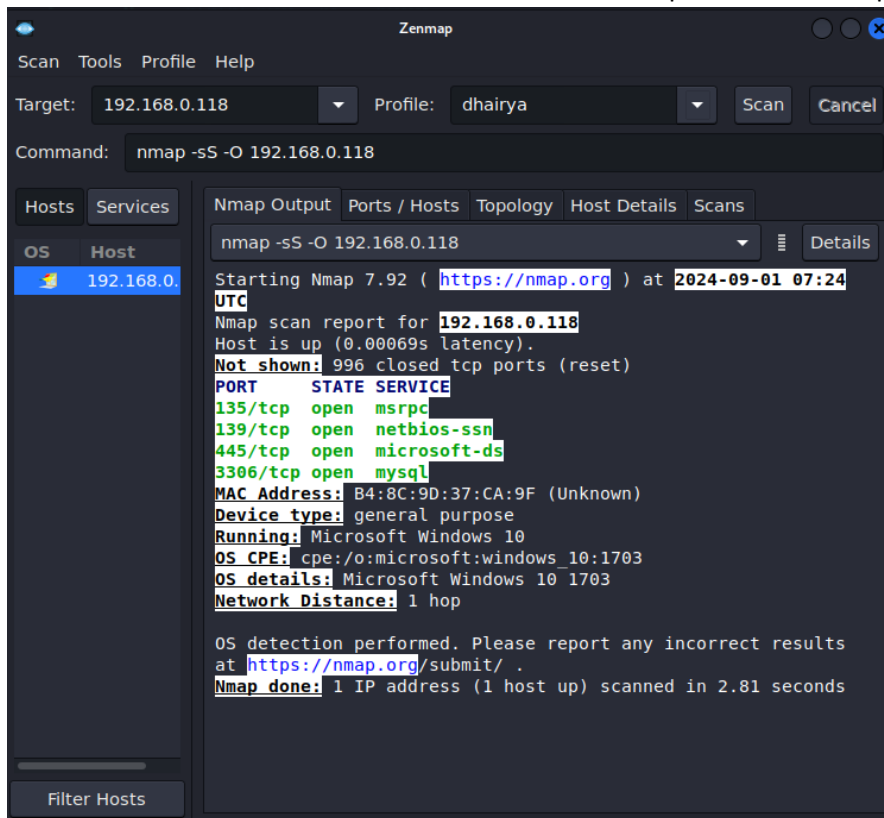
- Ping Scan: Only pings the target to see if it is online.



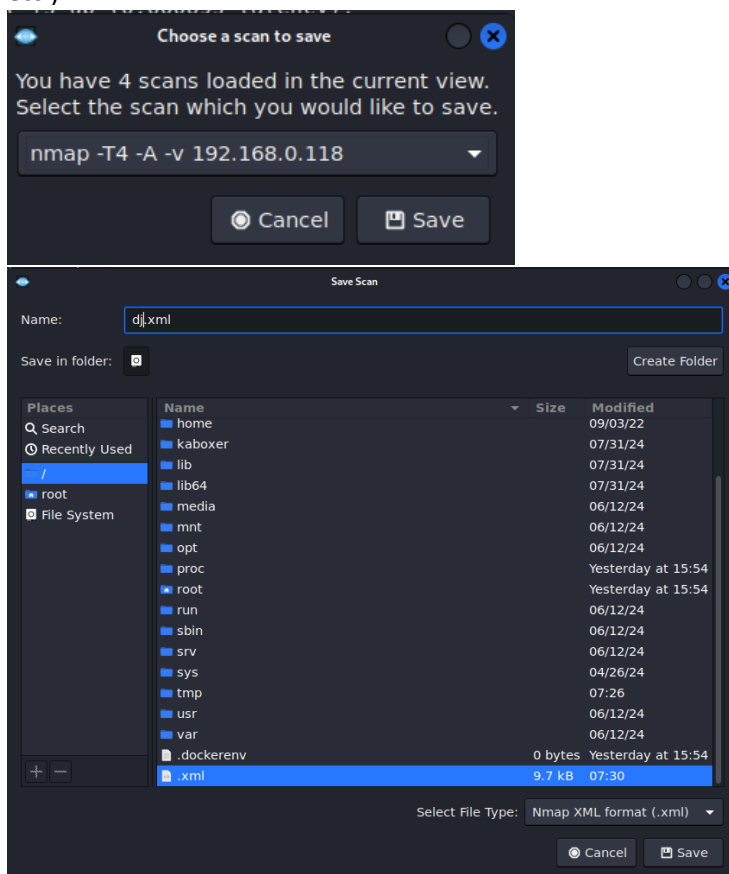
- Performing an Advanced Scan
- Use Custom Nmap Command
- perform a TCP SYN scan with OS detection:



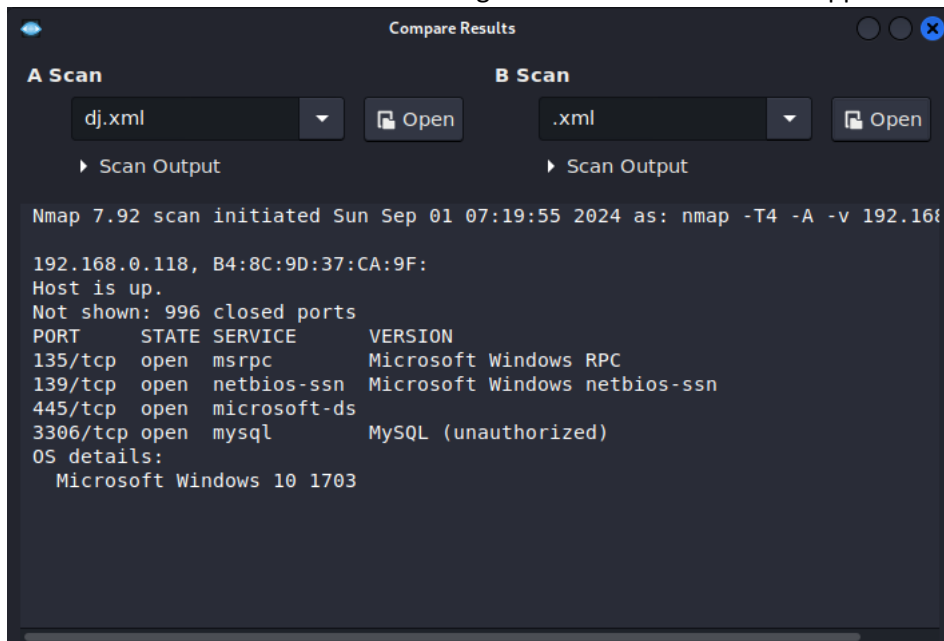
- Save Scan Profiles You can create and save custom scan profiles in ZenMap for future use:



- Saving and Comparing Results
- Save Scan Results After a scan, you can save the results in different formats (XML, Nmap output, etc.):

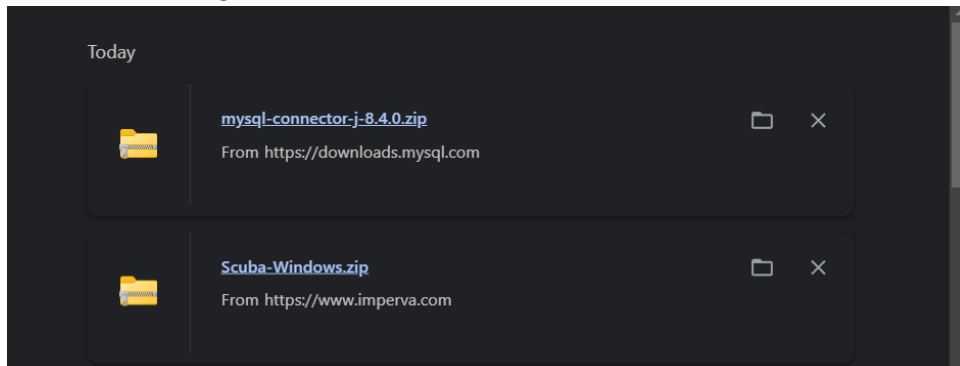


- Compare Results ZenMap allows you to compare the results of different scans to detect changes in the network. This is useful for tracking new hosts or services that appear over time.

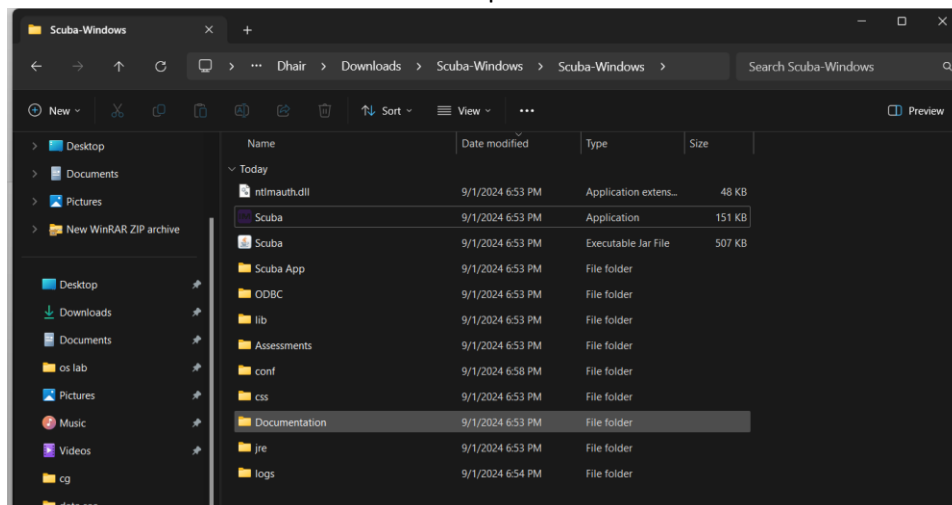


Aim- Database Scanning with Scuba

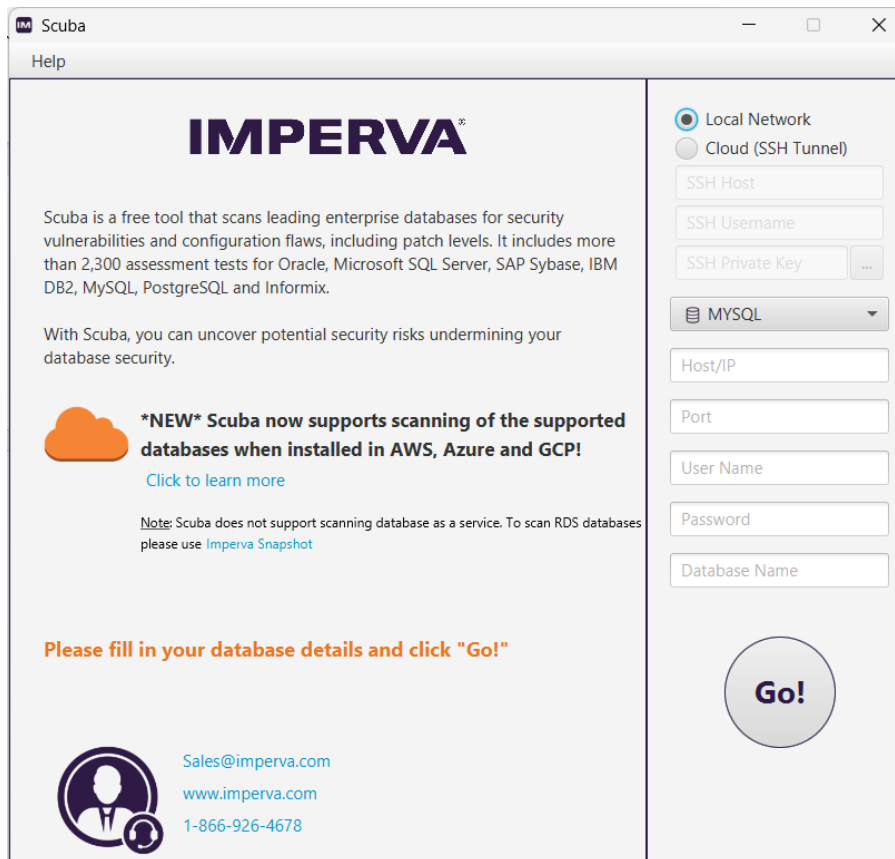
- Database Scanning with Scuba



- Install Scuba - Extract the downloaded zip file.



- Launch Scuba



The Scuba application window is titled "Scuba" and has a "Help" button. The main content area features the IMPERVA logo and a description of Scuba as a free tool for scanning enterprise databases. It lists supported databases: Oracle, Microsoft SQL Server, SAP Sybase, IBM DB2, MySQL, PostgreSQL, and Informix. A new feature announcement states that Scuba now supports scanning databases installed in AWS, Azure, and GCP. A note mentions that Scuba does not support scanning databases as a service and that users should use Imperva Snapshot for RDS databases. A large orange button labeled "Go!" is at the bottom right. The right sidebar contains configuration options for "Local Network" and "Cloud (SSH Tunnel)". The "Local Network" option is selected. Below it are fields for "SSH Host", "SSH Username", and "SSH Private Key". A dropdown menu shows "MYSQL" as the selected database type. Below the dropdown are fields for "Host/IP", "Port", "User Name", "Password", and "Database Name".

Scuba

Help

IMPERVA[®]

Scuba is a free tool that scans leading enterprise databases for security vulnerabilities and configuration flaws, including patch levels. It includes more than 2,300 assessment tests for Oracle, Microsoft SQL Server, SAP Sybase, IBM DB2, MySQL, PostgreSQL and Informix.


With Scuba, you can uncover potential security risks undermining your database security.

***NEW* Scuba now supports scanning of the supported databases when installed in AWS, Azure and GCP!**

[Click to learn more](#)

Note: Scuba does not support scanning database as a service. To scan RDS databases please use [Imperva Snapshot](#)

Please fill in your database details and click "Go!"

 Sales@imperva.com
www.imperva.com
1-866-926-4678

Local Network
Cloud (SSH Tunnel)

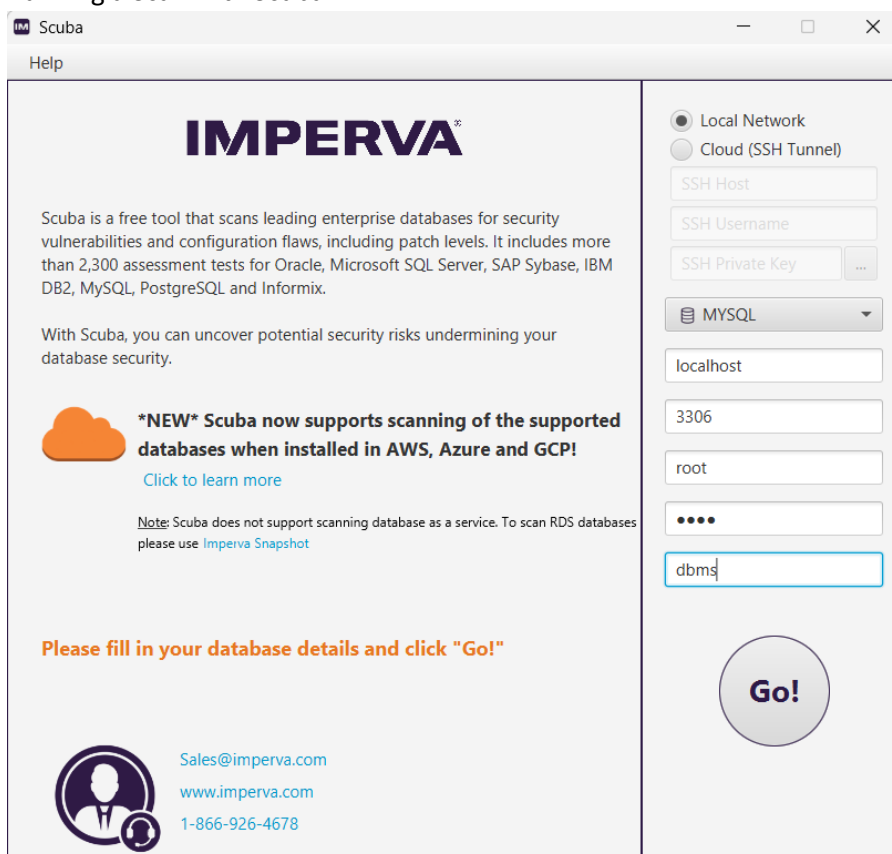
SSH Host
SSH Username
SSH Private Key ...

MYSQL

Host/IP
Port
User Name
Password
Database Name

Go!

- Running a Scan with Scuba



The Scuba application window is titled "Scuba" and has a "Help" button. The main content area features the IMPERVA logo and a description of Scuba as a free tool for scanning enterprise databases. It lists supported databases: Oracle, Microsoft SQL Server, SAP Sybase, IBM DB2, MySQL, PostgreSQL, and Informix. A new feature announcement states that Scuba now supports scanning databases installed in AWS, Azure, and GCP. A note mentions that Scuba does not support scanning databases as a service and that users should use Imperva Snapshot for RDS databases. A large orange button labeled "Go!" is at the bottom right. The right sidebar contains configuration options for "Local Network" and "Cloud (SSH Tunnel)". The "Local Network" option is selected. Below it are fields for "SSH Host", "SSH Username", and "SSH Private Key". A dropdown menu shows "MYSQL" as the selected database type. Below the dropdown are fields for "Host/IP", "Port", "User Name", "Password", and "Database Name".

Scuba

Help

IMPERVA[®]

Scuba is a free tool that scans leading enterprise databases for security vulnerabilities and configuration flaws, including patch levels. It includes more than 2,300 assessment tests for Oracle, Microsoft SQL Server, SAP Sybase, IBM DB2, MySQL, PostgreSQL and Informix.


With Scuba, you can uncover potential security risks undermining your database security.

***NEW* Scuba now supports scanning of the supported databases when installed in AWS, Azure and GCP!**

[Click to learn more](#)

Note: Scuba does not support scanning database as a service. To scan RDS databases please use [Imperva Snapshot](#)

Please fill in your database details and click "Go!"

 Sales@imperva.com
www.imperva.com
1-866-926-4678

Local Network
Cloud (SSH Tunnel)

SSH Host
SSH Username
SSH Private Key ...

MYSQL

localhost
3306
root
.....
dbms

Go!

- Reviewing the Scan Results

