**Introduction**: In this era of digital technology, people are more relying on computer applications than ever. As we are using them frequently, these applications are storing huge amount of our valuable data. And that’s why it has become one of the biggest challenges to protect these applications against any security threats and vulnerabilities. One single threat or vulnerability can expose all data from a network to the world-wide web and it’s too dangerous because it can hold sensitive information of users.

Network security tools are designed and used to protect a network infrastructure and its data from outside attacks. There are both software and hardware networking security tools which have different services like monitoring vulnerabilities and attacks from outside, scan for viruses, authenticate access and other security services. They are used in different purpose by different types of applications.

In this report, two types of open source software based network security tools are discussed with their brief description, installation procedure, a few features and an analysis based on their usability, performance, scalability and other terms.

**Tools Description**: We have selected two security tools, Wireshark and SqlMap. In this section, a brief description of these tools along with their purpose of use and their nature of services is presented.

* Wireshark: Wireshark is a free and open-source security tool which is used for network troubleshooting, network protocol analysis, different communication protocol development etc. This project originally started named as “Ethereal” in 1998 as open-source, meaning any developer is allowed to contribute to the software and it is also free to use [1]. That’s why it is regularly getting updates and becoming more robust as a packet sniffing tool. It is a multi-platform tool, so it can be installed and run on different operating systems such as Windows, Linux etc. The application has Graphical User Interface (GUI) as well as Command Line Interface (CLI). It is popular among networking people for live capturing network packets by filtering protocols and analyzing them online or offline. It is used for monitoring and analyzing network traffic, detecting bottlenecks and problems [2]. With the help of this tool, it is easy to determine the efficiency and manage the traffic of a network.
* SqlMap: SqlMap is also an open source network security tool which is used for penetration testing in order to detect and exploit SQL injection flaws and database vulnerabilities. It can simulate and perform SQL injection attacks to identify any vulnerability in the backend server. If a web server has vulnerable security protocol and allows SQL injection, it is possible to access and takeover the backend database and even underlying file system by executing commands on SqlMap. SqlMap has only command line interface (CLI) which allows to capture database information and perform database operations like upload and download files, enumerate users, password hashes, tables, columns, dump tables; if it is accessible. It has support for most of the popular databases like MySql, Postgre SQL, Microsoft SQL Server etc. and also different SQL injection techniques such as boolean-based blind, UNION query-based, stacked queries etc [3].

**Launching Tools**: In this section, we are going to demonstrate how to setup and launch these two tools on a Linux based machine using command line terminal step by step with screenshots. In this case, Ubuntu 18.04 is used as the Operating System (OS). But it is most likely to be very similar process in any other Linux based OS distribution. Ubuntu uses dpkg packaging system and Advanced Package Tool (APT) as a command line tool to handle the packaging system. APT provides services like installing, cleaning, updating and upgrading packages. So, we can download and install the security tools by APT commands from Ubuntu terminal. Installing procedure step by step is shown below.

* Wireshark:

1. Open up Ubuntu terminal.
   * Keyboard shortcut: Ctrl+Alt+T
2. Run this command:
   * sudo apt install wireshark
3. Running command with sudo means running the command with super user privileges, to install a new package with APT will require super user access. In order to access super user password should be provided.
4. It may ask for confirmation, whether or not to install and download the package, press enter or “y” to proceed. Terminal will show the progress.
5. It may take a while to download and install to the machine. Figure 1 shows the installation procedure.

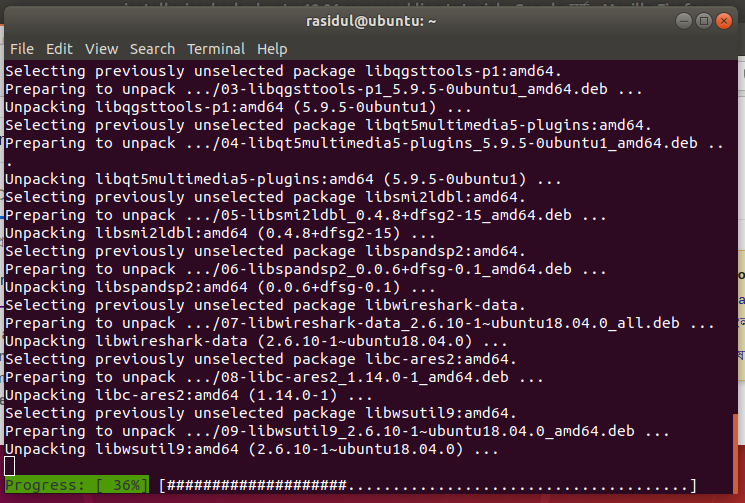
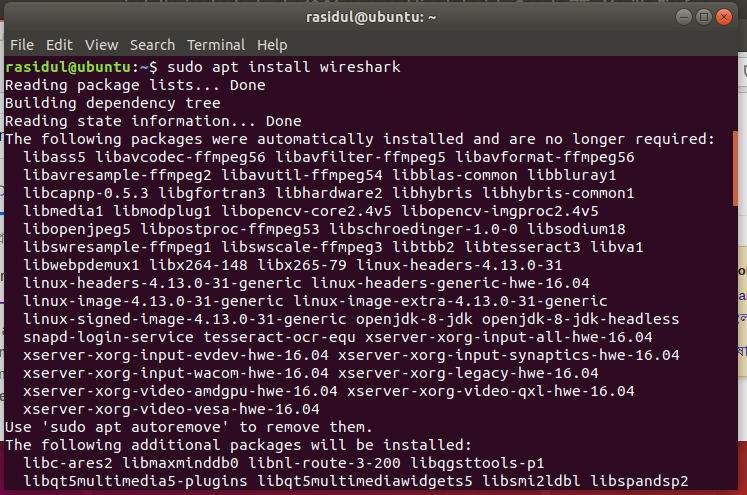


Figure 1: Screenshots of Wireshark installation from command line terminal.

1. Done.

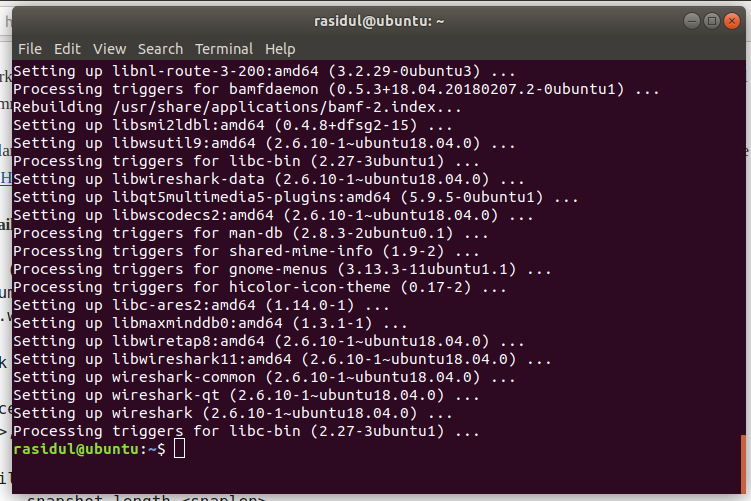


Figure 2: Wireshark Installation Completed

* SqlMap:
  1. Open up Ubuntu terminal.
     + Keyboard shortcut: Ctrl+Alt+T
  2. Run this command:
     + sudo apt install wireshark
  3. Running command with sudo means running the command with super user privileges, to install a new package with apt will require super user access. In order to access super user password should be provided.
  4. It may ask for confirmation, whether or not to install and download the package, press enter or “y” to proceed.
  5. It may take a while to download and install to the machine.

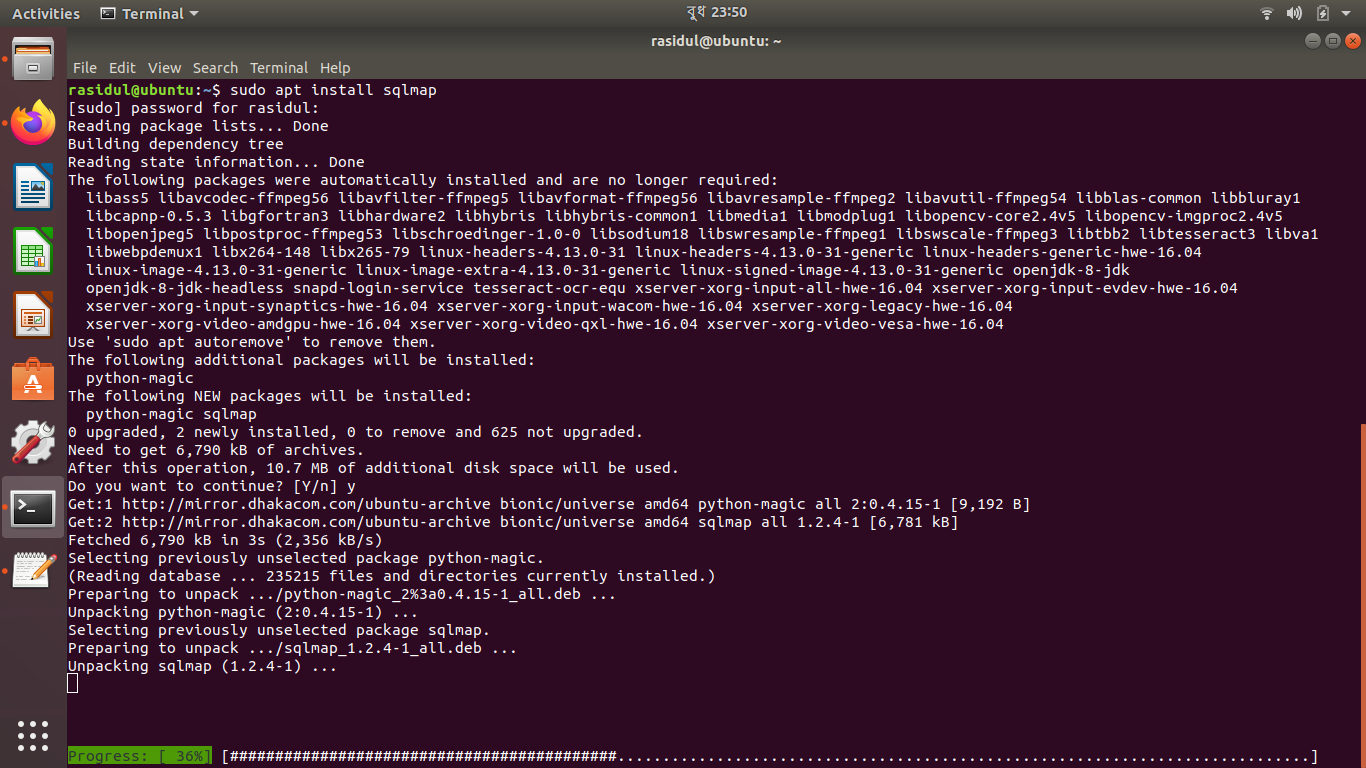


Figure 3: Screenshots of SqlMap installation from command line terminal.

* 1. Done.



Figure 4: SqlMap Installation Completed

**Evaluation**: In this section, an evaluation of a few features of each of the tools are demonstrated with a brief description and screenshots.

* Wireshark features:
  + Capturing data packets: We have tshark which is a terminal tool for wireshark to evaluate features. Figure 5 shows how to capture data packets by intercepting the packets that is crossing a specific node of the network.

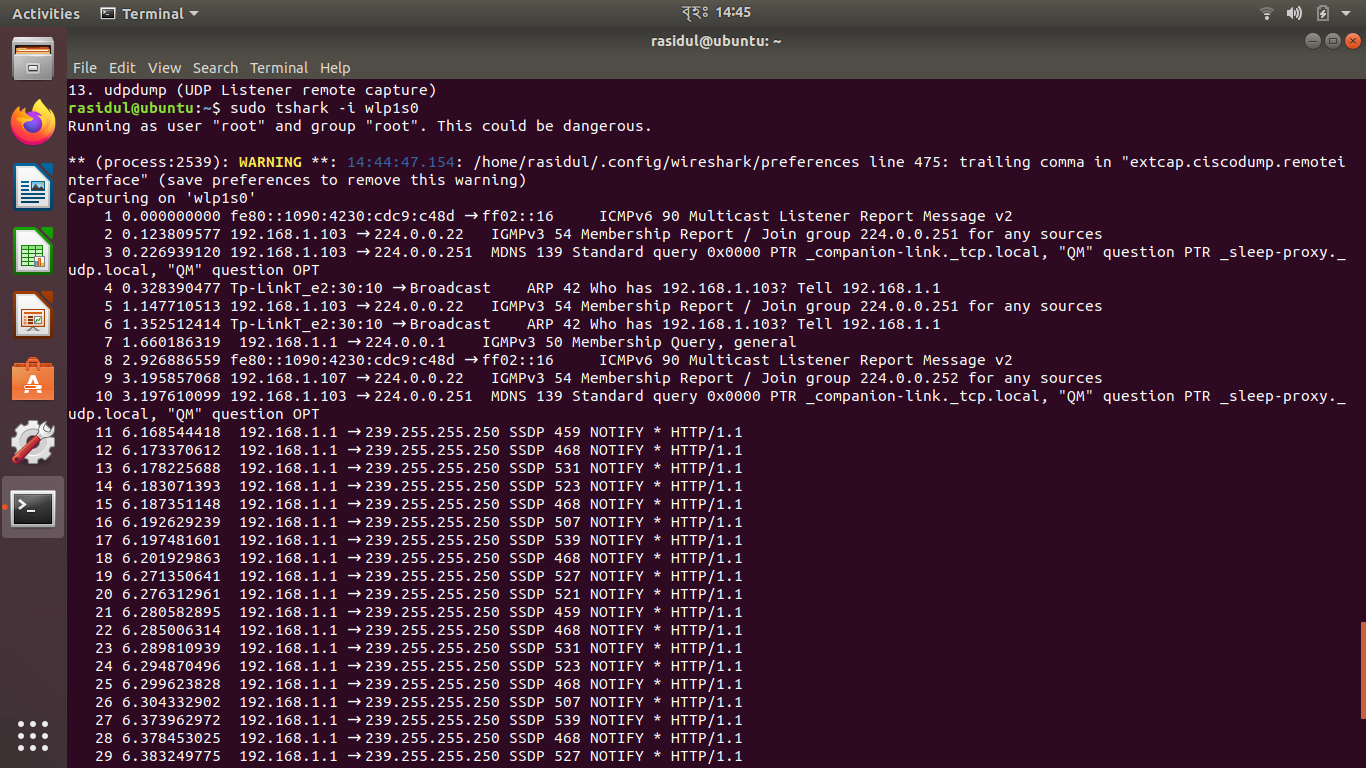


Figure 5: Capturing data packets

* + Filtering data packets: tshark, hence Wireshark provides extensive filtering options for the capturing process. Figure 6 shows how to capture packets coming from a particular host.

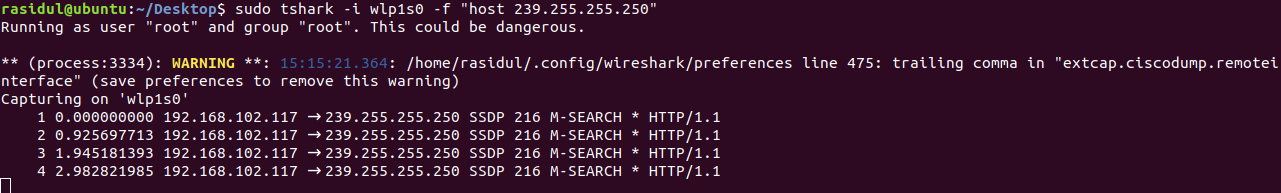
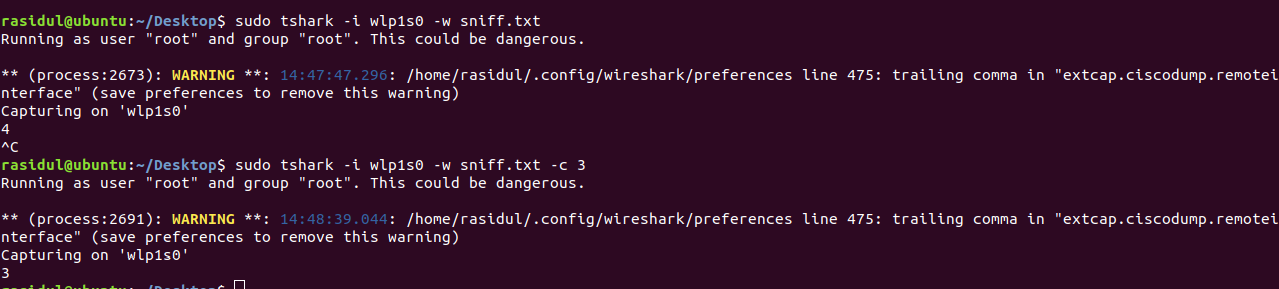


Figure 6: Filtering data packets

* + Export to file: These captured packets and their information can also be stored in a text file. Also we can limit the number packets we want capture and store.



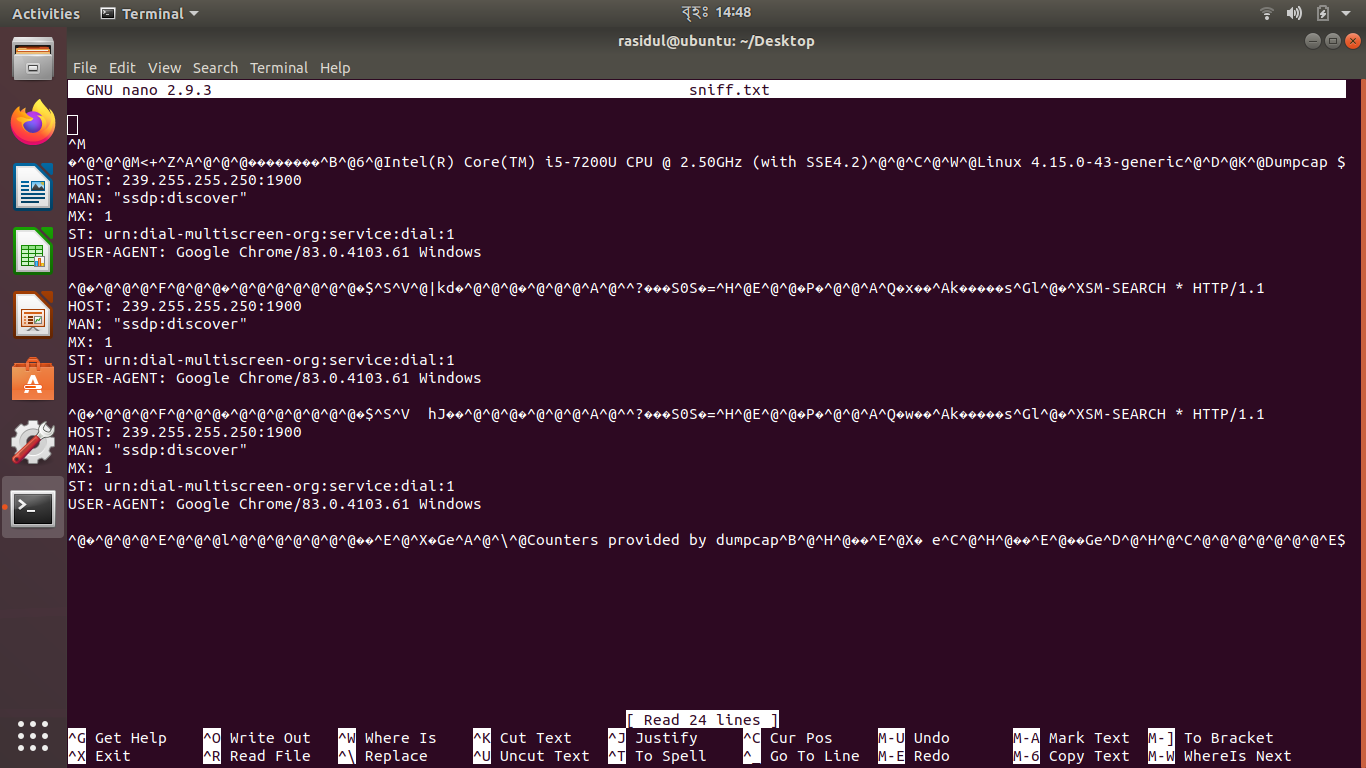


Figure 7: Capture and export data packet information to text file

* + HTTP analysis: We can perform http analysis by filtering out the http requests from different source and Figure 8 also shows from which browser and OS this requests are generating from.

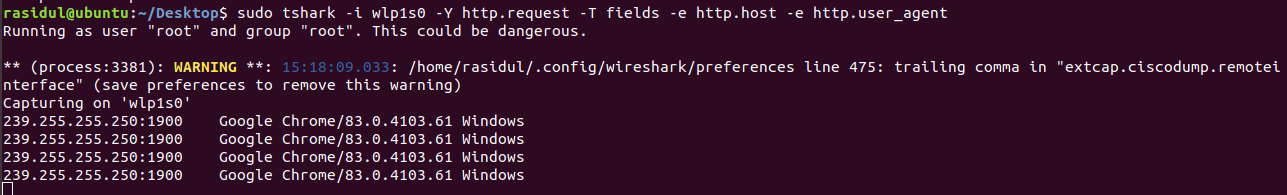


Figure 8: HTTP analysis

* SqlMap Features:
  + Capturing SQL injection flaws from websites: SQL injection attacks allow to inject code into any web based application in order to retrieve and manipulate data from the SQL databases [4]. But it is only possible to perform the operation if the server has vulnerability. That’s why SqlMap is a good tool which can provide detail information of vulnerabilities. In order to evaluate this, we picked a random website with vulnerability and run the command as follows:

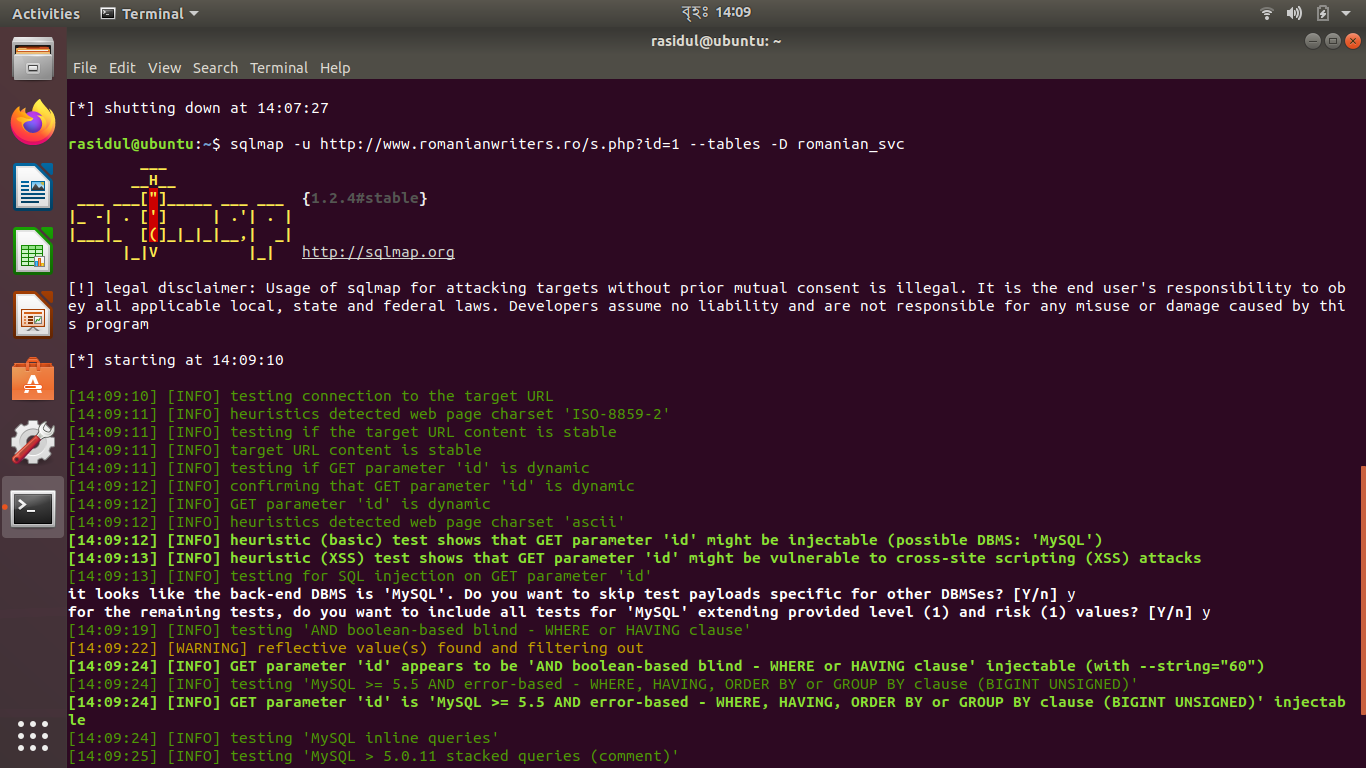


Figure 9: SQL injection flaws and vulnerability of the website

* + Getting web server and database information: If there are flaws and vulnerabilities in the server. It is possible to extract a few information of the server and database as well.

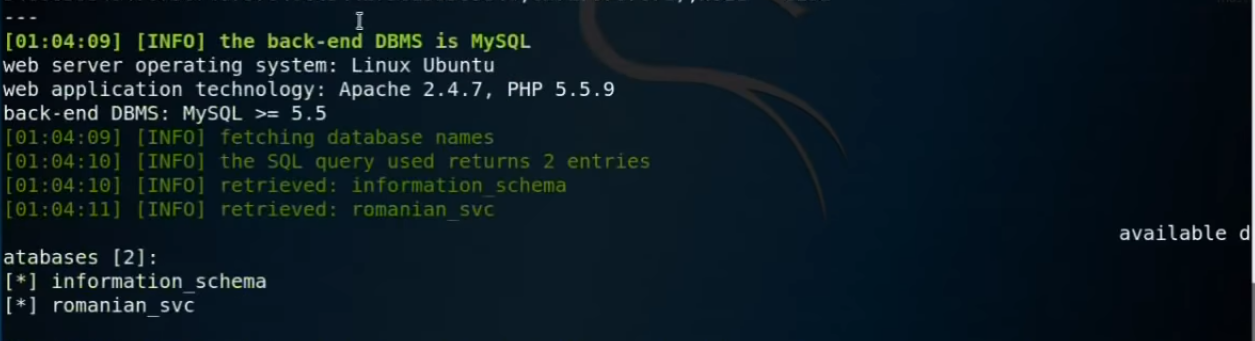


Figure 10: Web server and DBMS information captured by SqlMap

As we can see fig. 10 information of the web server and database system can be extracted from the vulnerable website by SQL injection technique.

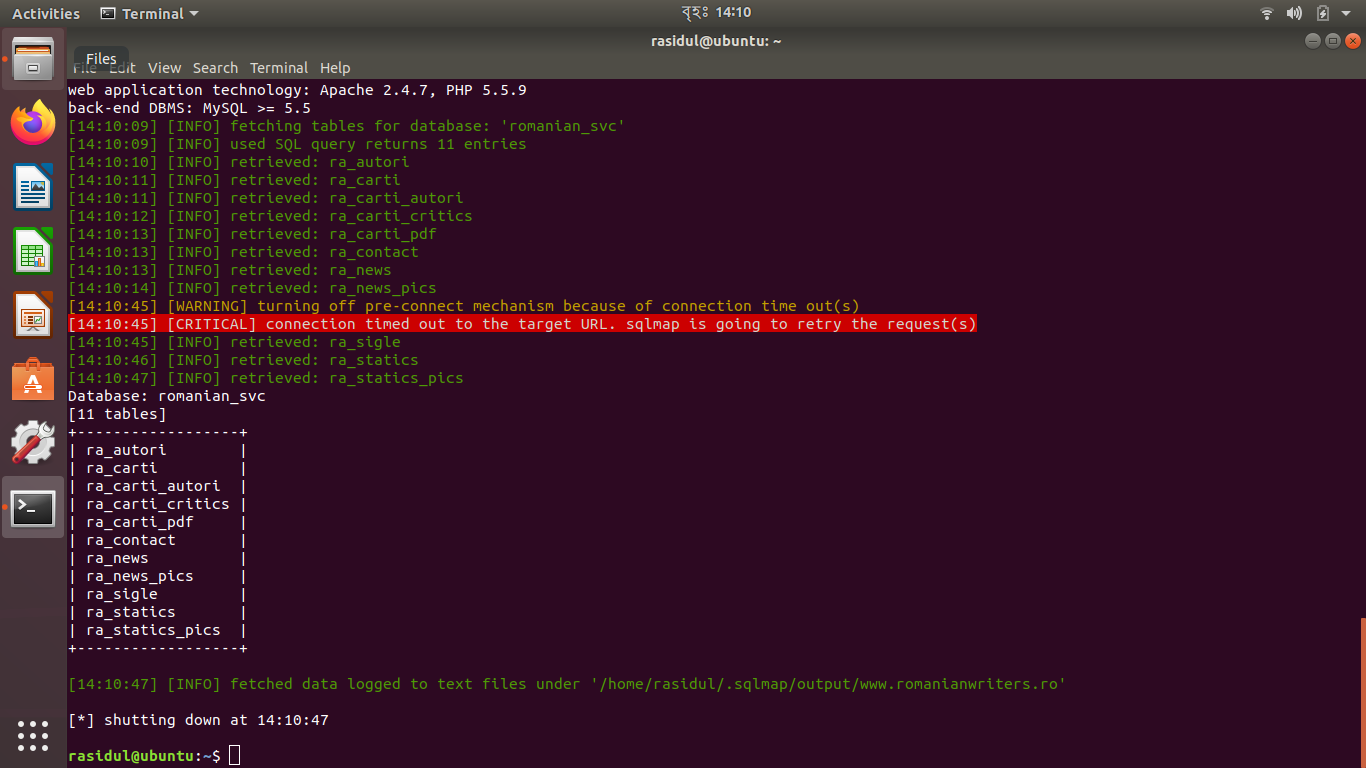
* + Getting specific table information of a database: SqlMap can provide database information with its table and column names as well.
  + 

Figure 11: Extracting table information from database

* + Dump table information and save into a text file: Figure 12 shows how we can dump all columns from a table from a database.

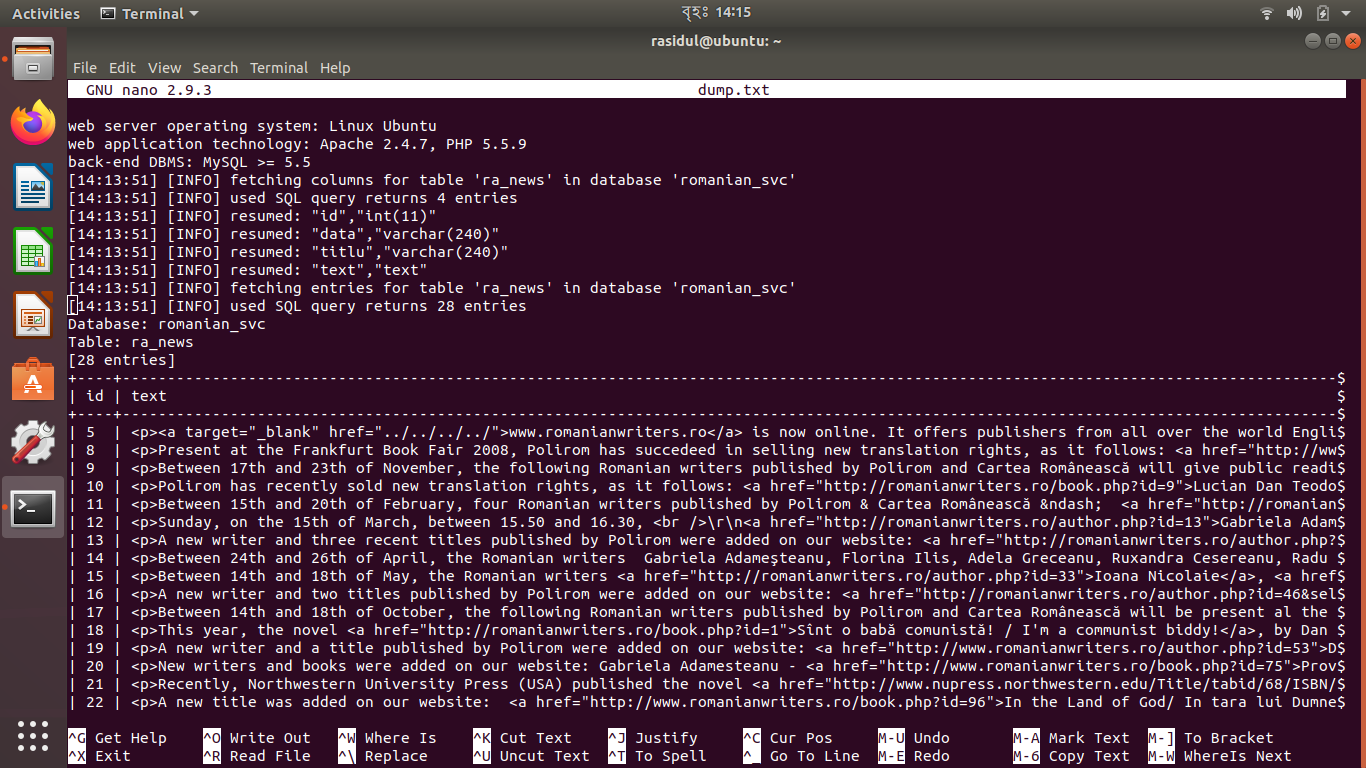
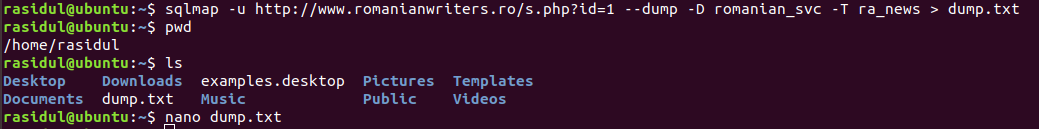


Figure 12: Save dump of particular table to a text file

**Analysis**: In this section, an analysis is presented based on a few criteria. Though Wireshark provides user-friendly GUI support, we used Ubuntu terminal (CLI) for both of the tools in order to evaluate and analyze their usability, performance, scalability, availability and reporting features.

* Ease of Use:
  + Wireshark is a very light-weight software with user-friendly commands. It doesn’t require high configuration to run on a machine. It runs very smoothly on a machine of 512MB RAM and requires only 500MB disk space [5]. Proper documentation and guidelines are also available. As it is a very widely used software by IT people and developers, there are forums to seek help and share knowledge. It is very simple to use, capture and filter network packets from any network adapter. It offers low-level extensive details of the packets with reporting tools to analyze data traffic in a network very easily. Though the CLI can be a little bit tricky for the non-technical person. But it also provides help command to show all the listings of available commands [1].
  + SqlMap is easy to use in command line interface to scan web application for vulnerability, penetration testing and database takeover [3]. It only requires simple commands with the URL of the website and can provide extensive information of the database. It also has massive online community of users for sharing the user experience.
* Performance:
  + Wireshark performs really well to collect network traffic and analyzing them. There are filters and search functionalities that can be applied both during capture and during analysis to filter out unwanted packets or find only the interested packets from the feed. In Wireshark, color codes can be used to identify different network packets based the types of the packets. This also helps the filtering process. Which makes the analysis more convenient and faster.
  + SqlMap is a powerful tool that can identify SQL injection vulnerability and takeover some access of the database if possible very easily. It has support for all of the most popular databases in order to analyze and get database information. It supports different techniques of SQL injection. Though the performance is not very satisfying among the users, a very common complaint is about its accuracy that it gives a lot false positive results, that means sometimes the tester has to manually check and confirm whether a detected vulnerability is actually exists or not.
* Scalability:
  + Wireshark allows to capture data packets and it is really fast. So, capturing data and exporting into file can be difficult as file size will be larger very quickly.
  + SqlMap can provide wide range of data from database of a vulnerable web server.
* Availability:
  + Wireshark is a free of cost, an open source software which can be found in Ubuntu APT. Also there are other sources where binary packages are available that can be downloaded and installed manually. It supports all the popular operating systems with easy installation, same features and functionalities.
  + SqlMap is operating system independent and free software. As it is developed in Python, it only requires Python interpreter version 2 or higher to install and run on a machine. It is very easy to find and install in any Linux distribution and also supports other OS.
* Reporting and Analytics:
  + Wireshark offers many integrated or embedded tools that can be used to perform more elaborated analysis such as HTTP, DNS and other filtering opetions. It also offers visualization and reporting tools.
  + SqlMap can provide detailed report of the backend databases by accessing directly with credentials. Full takeover of the database is also possible if the server is too much vulnerable.

**Conclusion**: These network tools can be used to monitor and identify network vulnerabilities and simulated to prevent the network from future security threats. Though they can provide extensive information and analytics, it is completely illegal to use them to perform security attacks to sensitive networks and it will be considered as cyber-crime. So, we need to remember that these are very powerful and useful tool but we have to make proper and safer use of them.

**References**:

[1] Wireshark Editorial, About Wireshark, [Online] Available:

<https://www.wireshark.org/about.html>

[2] S. Sandhya, S. Purkayastha, E. Joshua and A. Deep, "Assessment of website security by

penetration testing using Wireshark," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, 2017, pp. 1-4, doi: 10.1109/ICACCS.2017.8014711.

[3] SqlMap: Automatic SQL injection and database takeover tool, [Online] Available:

<http://sqlmap.org/>

[4] D. A. Kindy and A. K. Pathan, "A survey on SQL injection: Vulnerabilities, attacks, and

prevention techniques," 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE), Singapore, 2011, pp. 468-471, doi: 10.1109/ISCE.2011.5973873.

[5] Wireshark System Requirements, [Online] Available:

<https://www.wireshark.org/docs/wsug_html_chunked/ChIntroPlatforms.html>