|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Submission Coversheet (All Programmes) | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **Student ID Number**  *(Do not include student name as anonymous marking is implemented)* | Radu Garaz/GAR19472838 | | | | | | |
| **Programme Title** | Computing Technologies Extended Degree (QA) | | | | | | |
| **Module Title** | Web Application Security | | | | | | |
| **Module Code** *(listed on Moodle and in LTAFP)* | QAC020N256S | | | | | | |
| **Module Convenor** |  | | | | | | |
| **Coursework Title** | Assignment 1 | | | | | | |
| **Academic Declaration:**  *Students are reminded that the electronic copy of their essay may be checked, at any point during their degree, with Turnitin or other plagiarism detection software for plagiarised material.* | | | | | | | |
| **Word Count** |  | | | **Date Submitted** | |  | |
|  |  | | |  | |  | |
| Please save your file as:  student id\_module code\_module\_title\_assessment name  for example: COR15416549\_QAB020N592S\_Managing Organisations)\_Essay 1 Teamwork | | | | | | | |

**Table of Contents**

[**Introduction 2**](#_Toc27927)

[Background 2](#_Toc26971)

[**Aim 2**](#_Toc7972)

[**Set up a fully functioning Web Applications 3**](#_Toc28671)

[Virtual Box Installation 3](#_Toc4351)

[“Configuration details of the environment setup XAMPP/WAMP” 8](#_Toc29881)

[**Advantages of XAMPP/WAMP: 9**](#_Toc12553)

[Web/application and back-end database 14](#_Toc21136)

[Mutillidae Installation 16](#_Toc972)

[**Web Application Security Testing 20**](#_Toc8975)

[Nmap scanning 20](#_Toc3852)

[Wireshark Sniffing 26](#_Toc1462)

[SQL Injection using SQLMAP 31](#_Toc27143)

[**Design and Implement a web security model 34**](#_Toc15256)

[IDS/IPS 34](#_Toc1293)

[Firewall 35](#_Toc294)

[Antivirus 36](#_Toc2721)

[**References 37**](#_Toc8009)

# Introduction

## Background

The COVID-19 epidemic has altered humans's perceptions of truth and brought on numerous, in addition to individuals of the more youthful generation, to pay longer online than they antecedent had. In their eyes, the internet may be a boon to society and one several the primary dependable and low in cost manner that of acquiring our thoughts through, especially as soon as it entails our private and professional lives. On the alternative aspect, the Internet's arrival, and lots of programs rectangular degree generally visible at some stage in a bad lightweight. As a result, cyber hectoring, numerous humans and agencies rectangular degree left feeling confused. Often, humans do now no longer apprehend what they're experiencing is blustering. As a result, the as soon as-secure internet placing is presently a delivery of issue and obfuscation for plenty folks. As a result of this brief growth, one out of every 4 agencies have observed a cyber safety breach inside the previous couple of months of operations. As a result, several organizations are likewise unaware that their IT structures are compromised and need to know no longer expertise to manipulate or prevent such assaults. London-primarily based totally Prohunt may be an assets' funding trust. Residential and commercial enterprise homes inside the location rectangular degree treated through this commercial enterprise, that rents, purchases, and sells them. They're committed to giving the handiest doable provider to their customers. 2 administrators, 2 receptionists, 4 place of business directors, 2 consultants, and seven discipline employees conjure the employer's force. Prohunt plans to decide its employer online, giving one-prevent property services, to stay aggressive and fashionable. It's the intention of this new internet site to create it less complicated for customers to test in for their products and services, in addition on reduce the variety of a while spent on tedious frame activities. It's few mysteries that this generation can facilitate the membership save money and maintain financially sound while conjointly improving consumer provider, defensive purchaser expertise, and lowering safety threats.

# Aim

As an end result, "ProHunt" has reached out to BuildTech (a main IT employer) to have their internet site's safety checked a good way to painting their on line presence and services. As a way of conversation with its consumers, the consumer can even make use of the internet site. A safety audit of your consumer's internet site and the SQL database related to it's been assigned to us, and your reaction might also additionally make honest assumptions approximately the findings of that audit.

# Set up a fully functioning Web Applications

## Virtual Box Installation

Virtual-Box is a cross-platform, open-source virtualization software. It allows you to run Linux on your Windows computer. It runs inside a window on your computer but looks and acts like a separate computer. You can install and run multiple operating systems, including Linux, Mac OS X and Windows operating systems.

Before installing Virtual-Box, make sure that your computer meets the hardware requirements for using Virtual-Box. If you have an old computer with very little memory (RAM) and processor speed, running more than one operating system simultaneously will be very slow. You will need at least 512 MB of RAM to run Virtual-Box. If you plan to use newer operating systems such as Mac OS X or Windows 7, you will need 1 GB or more of RAM to get decent performance.

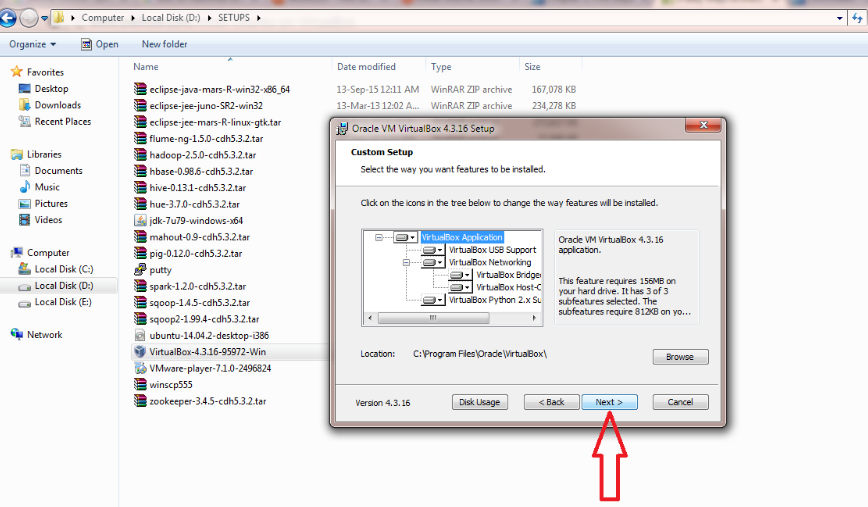
Run the Virtual-Box-4.3.16-95972-Win.exe application. You will have the Oracle (VM) Virtual-Box Installation dialogue box.

Instructions for Set up Virtual-Box

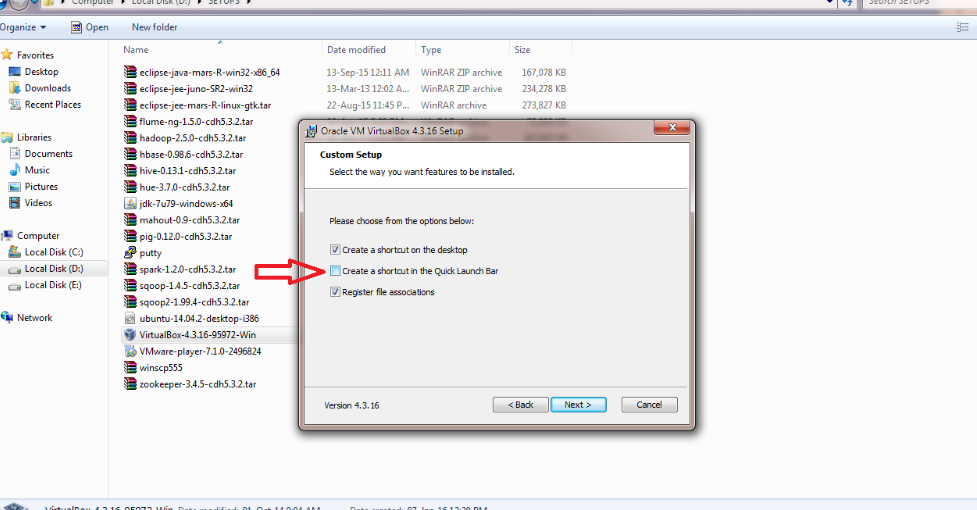
Virtual-Box may be set up in a rely of mins the usage of those easy commands and pictures. You can without problems set up Virtual-Box in your laptop with the useful resource of the screenshots available below.



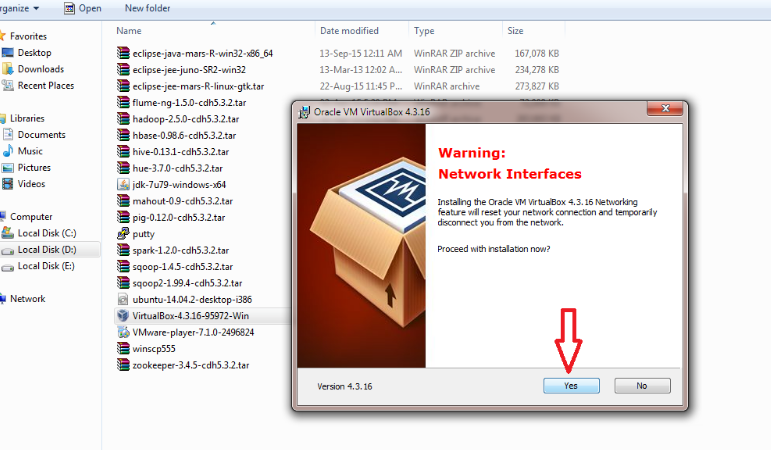
Click Next



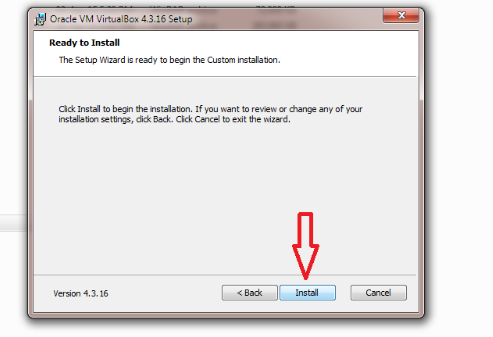
Un-check “Create a shortcut in the Quick Launch Bar” and click “Next”



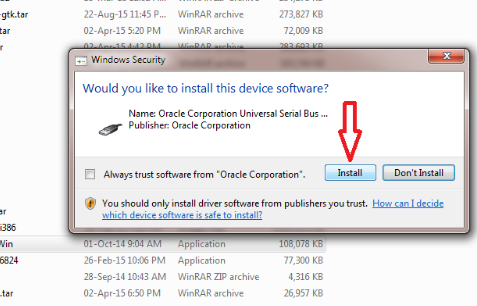
Click “Yes”



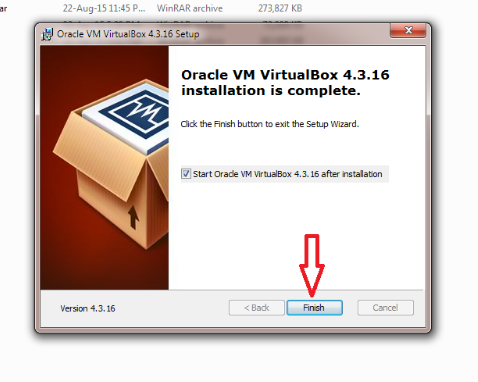
Click “Install”



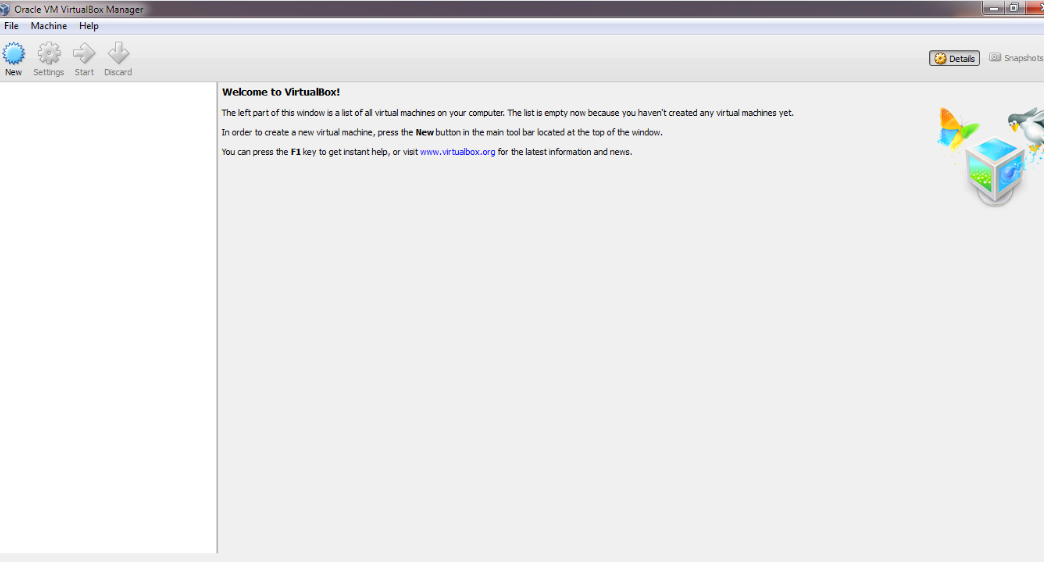
Click “Install”



Click “Finish”



when the installation is complete open Virtual-Box's window.



Click “Start button” on your taskbar to start Virtual-Box. After deciding to use a bridged adapter, click on Change Network Settings.

To finish the operation, we will need to establish a username and password.



****

## “Configuration details of the environment setup XAMPP/WAMP”

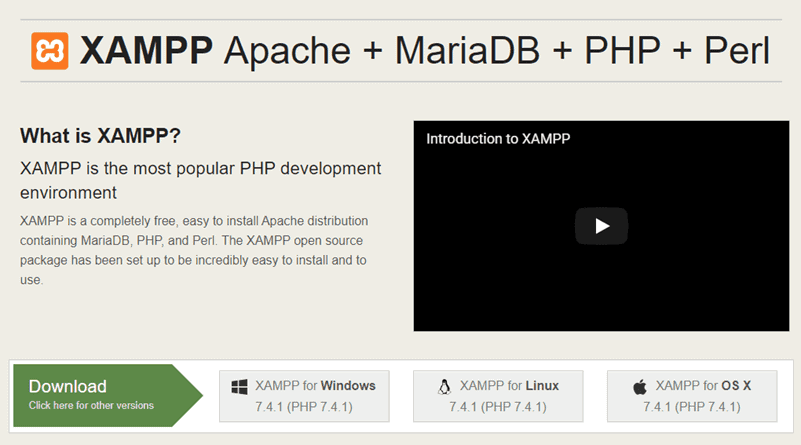
XAMPP and WAMP are Apache web hosting packages. When you install them, no matter what you do, they include settings that change your Apache configuration. Sometimes it's bad, so you have to change them; sometimes it's good, and in general it's very important for security reasons.

For example, when you set up a site with XAMPP or WAMP (or any other Apache server), the settings are configured to use port 80 instead of port 8080. This is what the TOS page says. It was a feature when I was setting things up, and I didn't think about it until I read the manual, but then I thought "Wow! That's a terrible idea!"

If someone managed to intercept your connection and replace port 80 with port 8080, he would be able to view every page on your site. He would also be able to serve pages of his own on the same port 8080 address.

You can avoid this by using www-data or nobody as the username; nginx will give a warning if you try to set the user name explicitly.

I will intimate you to avoid Apache; it's wonderful software.



XAMPP stands for Cross-Platform (X), Apache (A), MariaDB (M), PHP (P) and Perl (P). It is a simple, lightweight Apache distribution that makes it extremely easy for developers to create a local web server for testing purposes.

WAMP stands for Windows (W), Apache (A), MySQL (M) and PHP(P). It allows you to create web applications with Apache2, PHP and a MySQL database. Alongside, PhpMyAdmin allows you to easily manage your databases.

# Advantages of XAMPP/WAMP:

1.Simple installation process

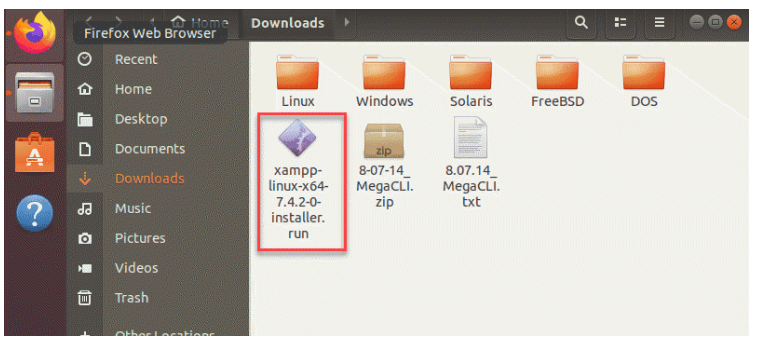
2.Does not require any additional configuration

3.It allows you to have multiple versions of PHP installed at the same time

4.It has a great community support

5.The latest version includes all the necessary components:Apache,MySQL and phpMyAdmin





“To make the newest XAMPP installation package executable, use the instruction:

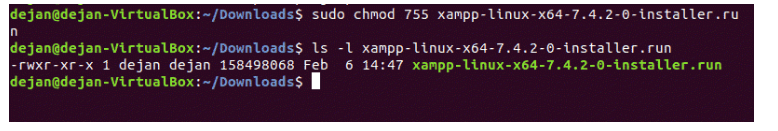


The concluding does not give any verification nor output that you have successfully executed the above step. However, verify you have run the permission with the command:



The output must incorporate rwxr –xr –x 1 incorporate by the name of the user who can now run the file,

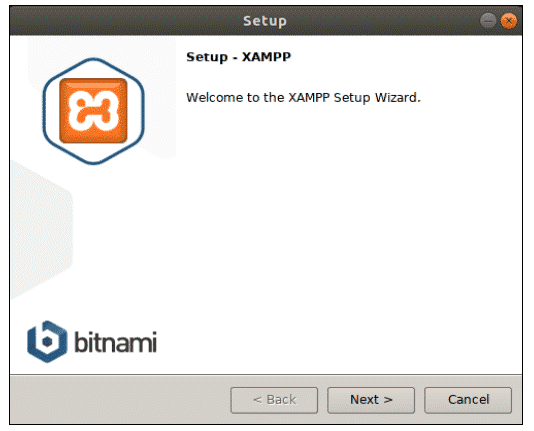
As in the image below:”



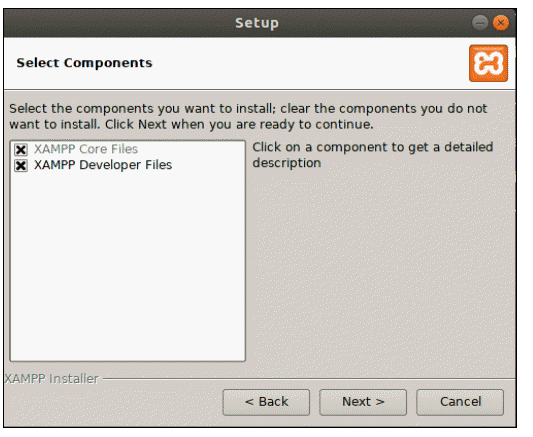
Now execute the installer and launch the graphical framework wizard with the following instructions:



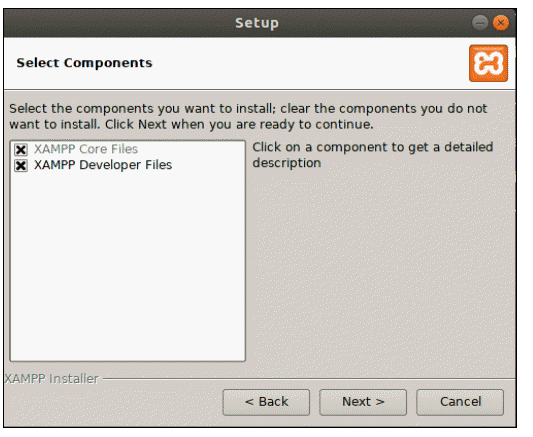
The XAMPP system Wizard opens in a new window on top of the end that will display as in the following image:

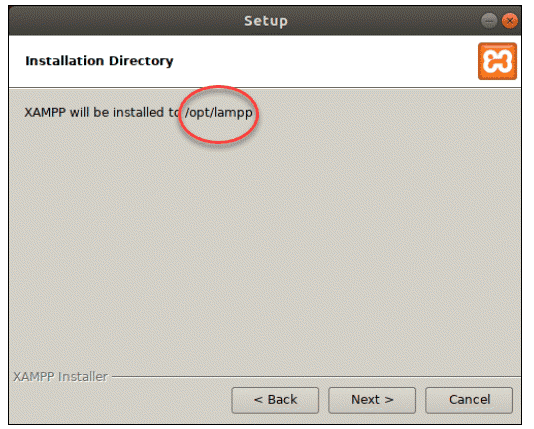


Click Next



Click Next.

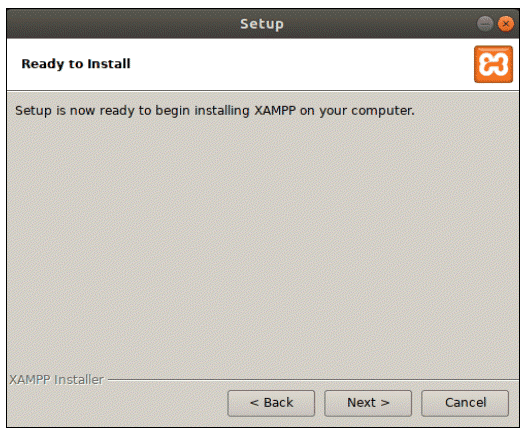




Click Next



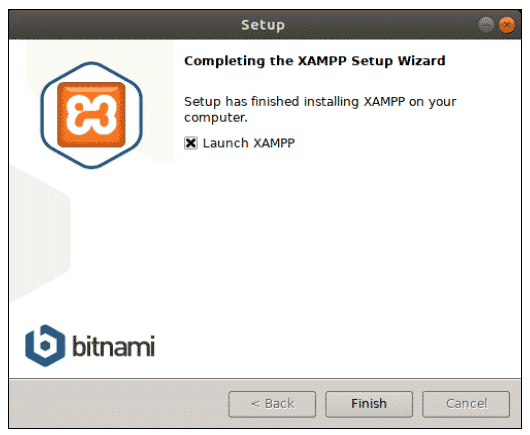
Ready to Install the XAMPP server.



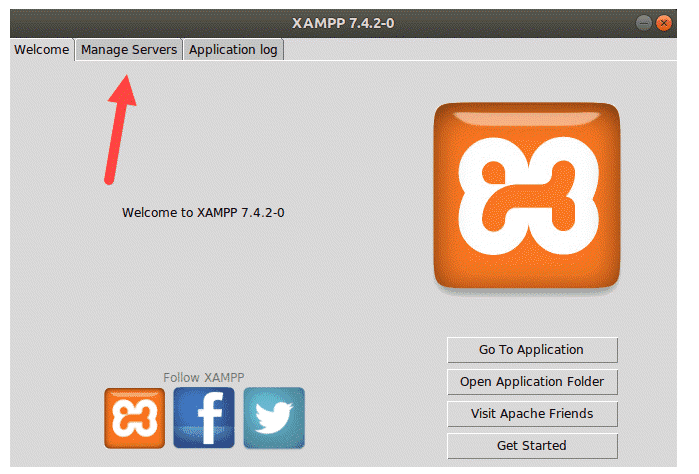
Installation



“The final dialogue box should display that the setup has finished installing. You can complete the process and launch XAMPP by clicking **Finish.**



Click finish

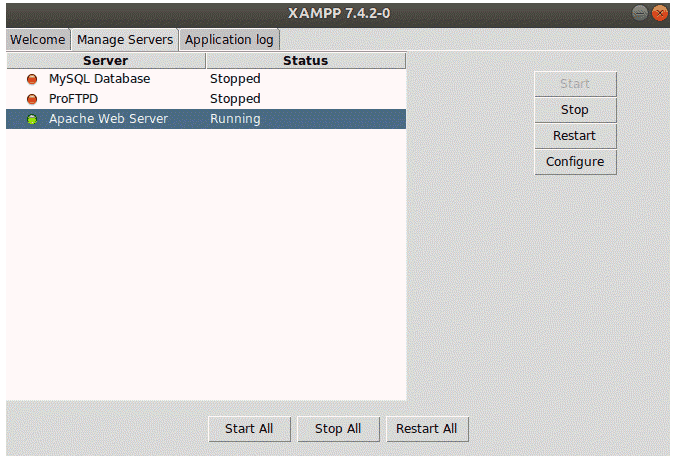


## Web/application and back-end database

For a full-stack developer, it's beneficial to understand the different architecture of a web application or website. The most popular architecture is usually called LAMP. It stands for Linux, Apache, MySQL, and PHP.

The Linux operating system is what hosts the web server software (Apache), the database engine (MySQL) and the programming language (PHP). PHP code is what generates the HTML pages to be served to the client. The MySQL database engine stores all the information.

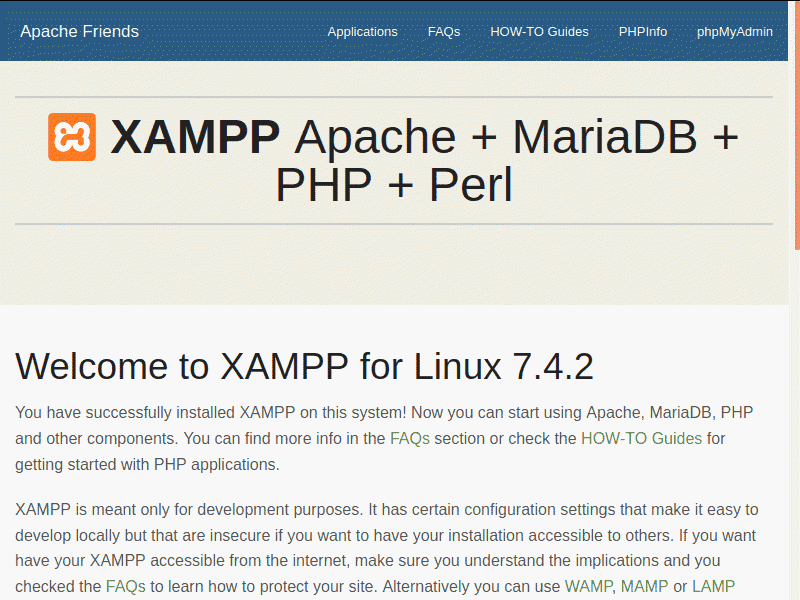
Open the Manage Servers to visit all the facility and status.



Checking XAMPP by entering the URL given below

<http://localhost/dashboard>

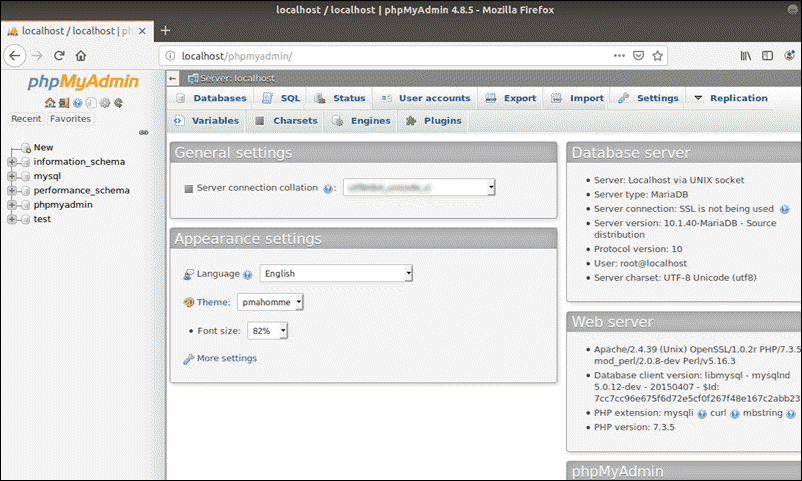
If it is successfully installed, then it will display the dashboard



Next, confirm whether the MariaDB service is working. To do so, open the URL:

**http://localhost/phpmyadmin**

The output screen for a properly working database service should appear as:”



## Mutillidae Installation

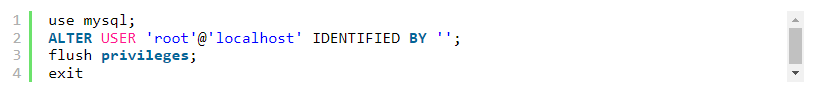
Mutillidae is a free, open-source web application provided to allow security enthusiest to pen-test and hack a web application. Mutillidae can be installed on Linux and Windows using LAMP, WAMP, and XAMPP. Although typically installed on a PC for security testing, Mutillidae is designed to be vulnerable intentionally so it can be hacked for learning purposes. Mutillidae is intended to teach web application security by showing examples of common vulnerabilities in deliberately vulnerable code. This project takes the OWASP Top 10 list and uses examples from each of the Top 10 vulnerabilities in the project code.

As of MySQL 5.7, log-in as the root-user requires the use of “sudo” command, a new and secure paradigm. Mutillidae II and Damn Vulnerable Web Application (DVWA) are incompatible with these settings.

To utilise the MySQL / MariaDB database without requiring sudo rights, just log in as an ordinary user at the MySQL command prompt.



“Run the following instructions:



Then restart the MySQL service:



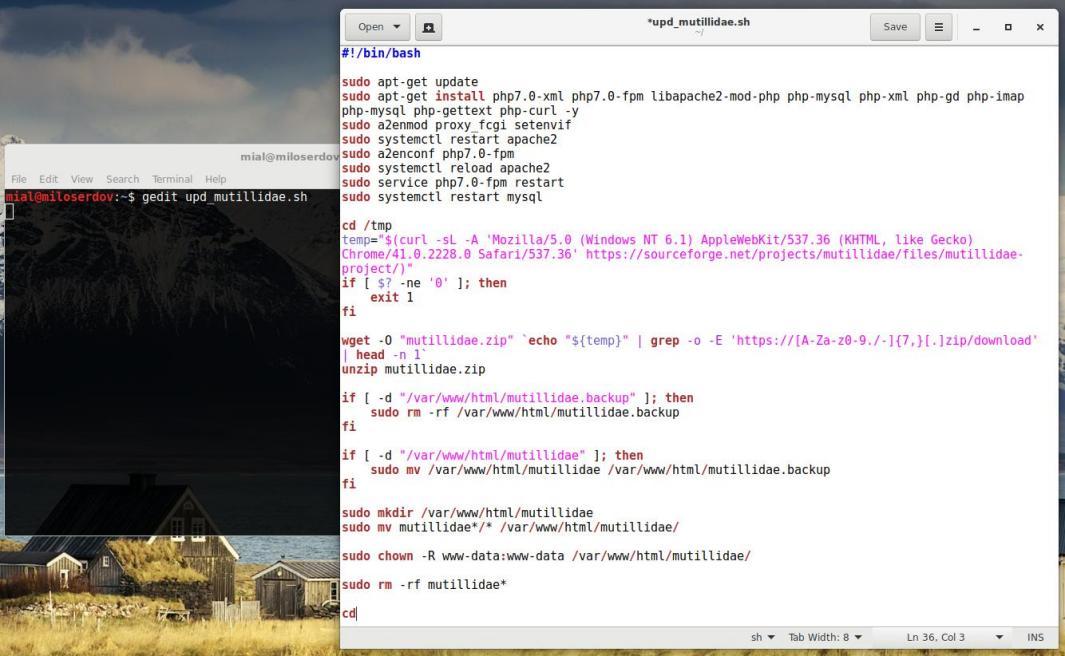
Create a family database,



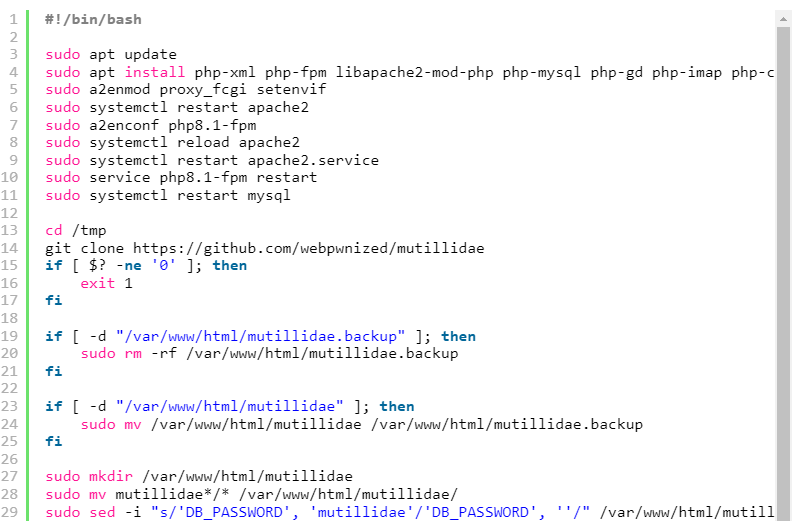
And execute



Create a file **upd\_mutillidae.sh**:



and copy-paste the script into the created file:”

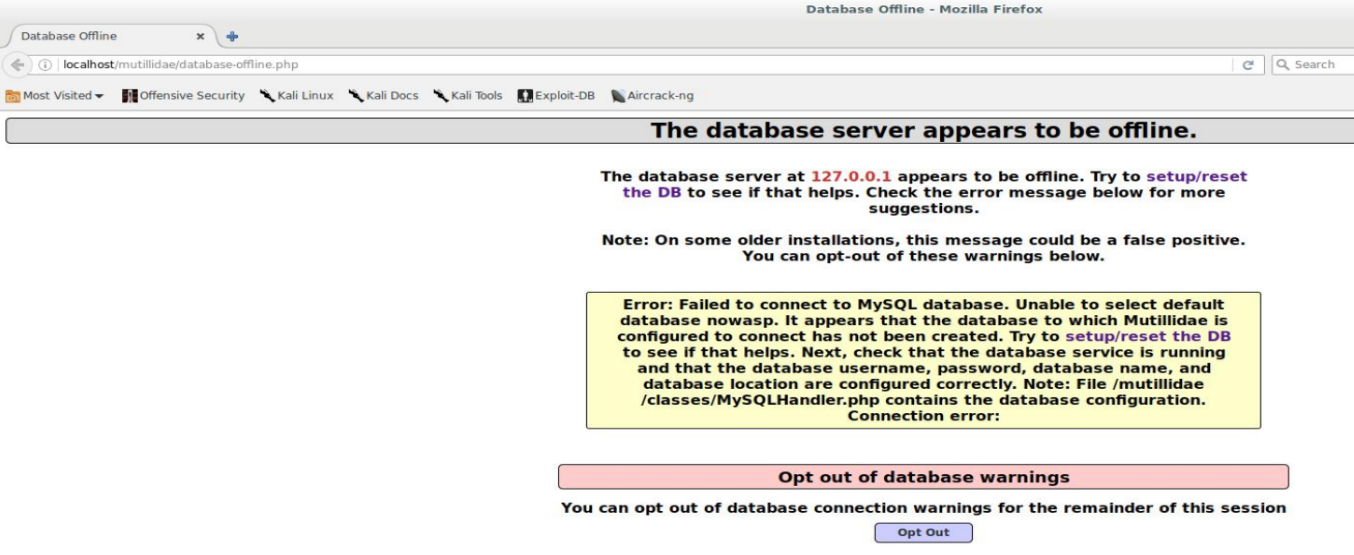


“Execute the script:

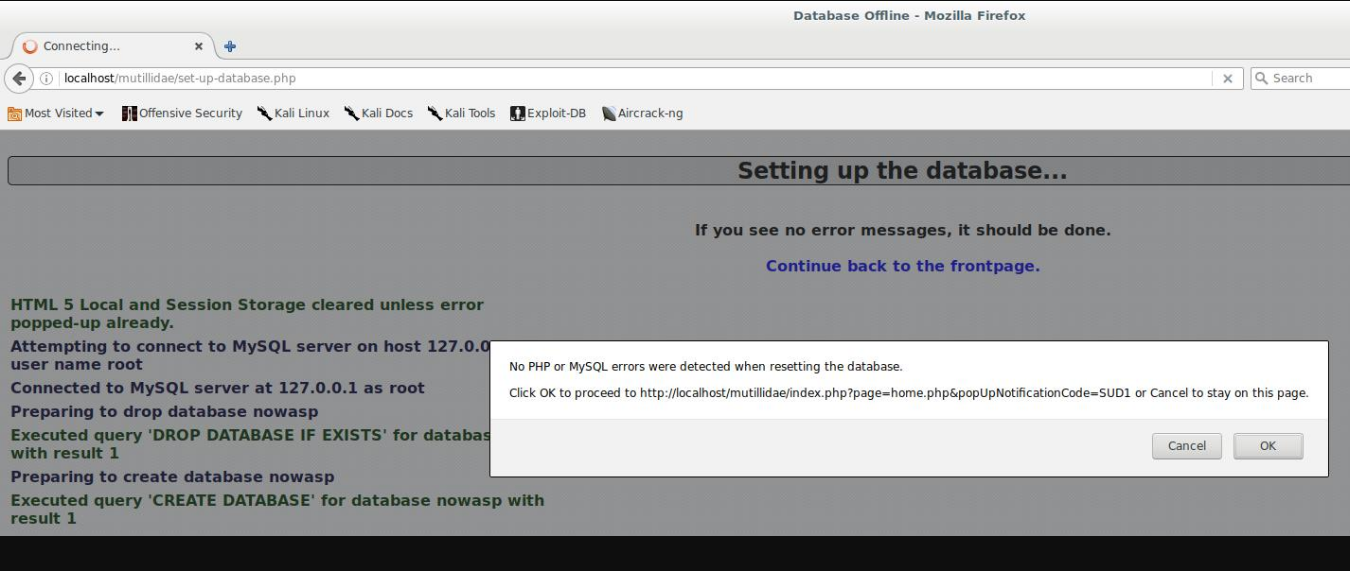


OWASP Mutillidae II is accessible at

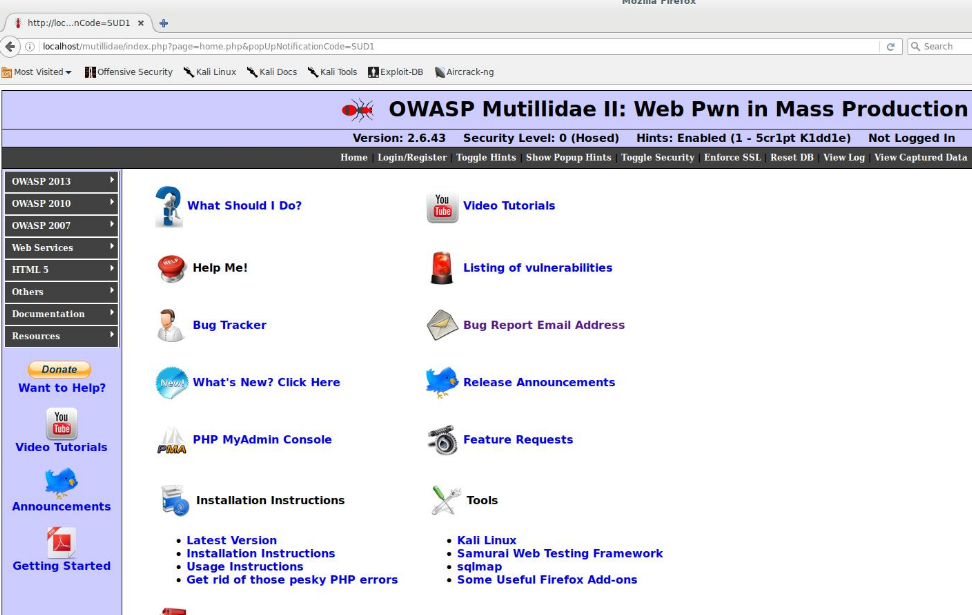
<http://localhost/mutillidae/>



“Click «system/reset the DataBase»



To initiate the database system, follow the link: <http://localhost/mutillidae/set-up-database.php>”



# Web Application Security Testing

Web application security testing is a process of identifying the loopholes in web applications to ensure that they are secure and protected from malicious attacks. Web applications have vulnerabilities and these vulnerabilities when exploited could lead to severe consequences such as data theft, loss of reputation and revenue, etc.

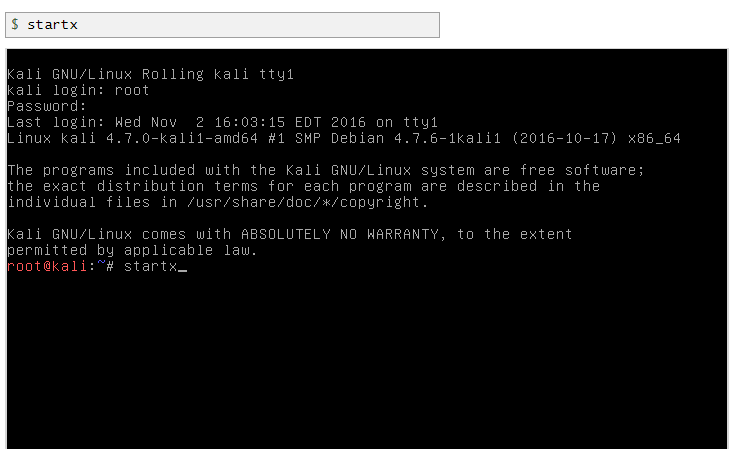
Web application security testing is a systematic process for identifying the potential threats and vulnerabilities in web applications. These tests are carried out by ethical hackers using white box approach, where internal structure of the web application is known (or) black box approach, where internal structure of the web application is not known.

## Nmap scanning

Nmap is a network scanning tool. To scan a network is to interrogate the various devices on the network and find out which ones exist, what IP addresses they have and what services they are offering. Services are typically things like web servers, email servers and so on.

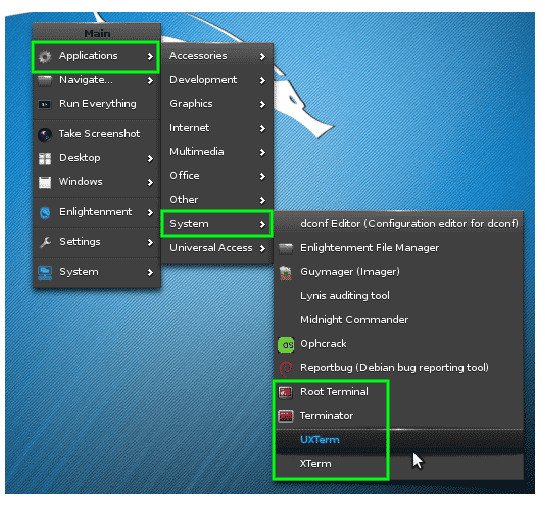
Nmap uses raw packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

To get access to Kali Linux, you'll need to submit the system's root password. Enlightenment is a desktop environment that may be used on Kali Linux after logging in. Even without a desktop environment, Nmap can do its tasks.



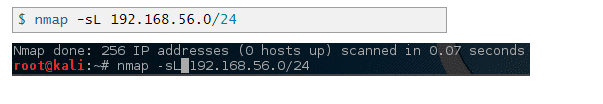
Now need to start a terminal window.

When you click on the desktop wallpaper, a menu will display. Applications –> System –> “Root Terminal”.



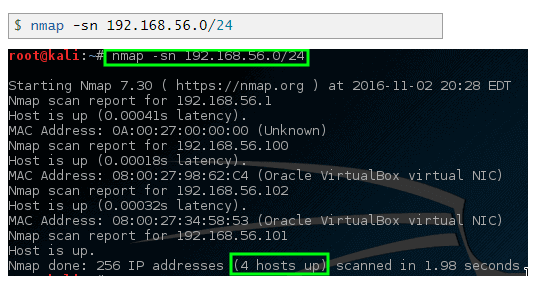
### All shell codes do work for causes of the Nmap module of Linux.

The IP # of the kali machine is 10.0.2.15, and the IP # of the machine is ‘192.168.56.102’.



“Find and query All Live hostess on My Network:

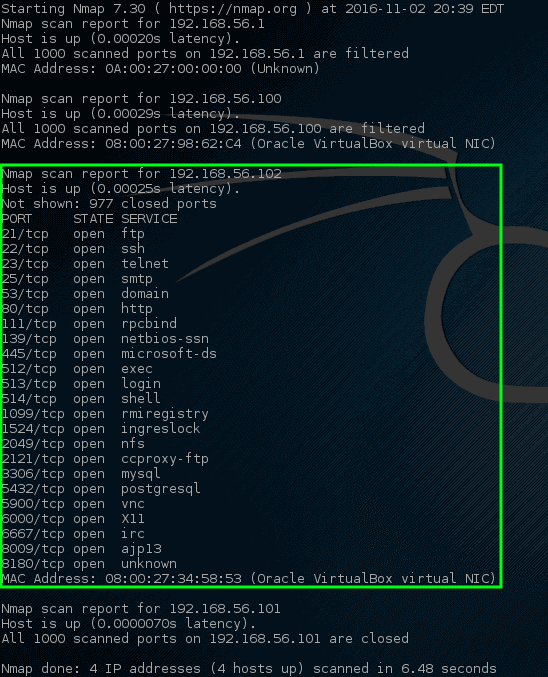
We can determine these machines. Method and trick will specify Nmap to state all IP# in the 192.168.56.0/24 network.



### Find open ports via Nmap:

Let Nmap do a scan for port to find particular targets and see the results.”



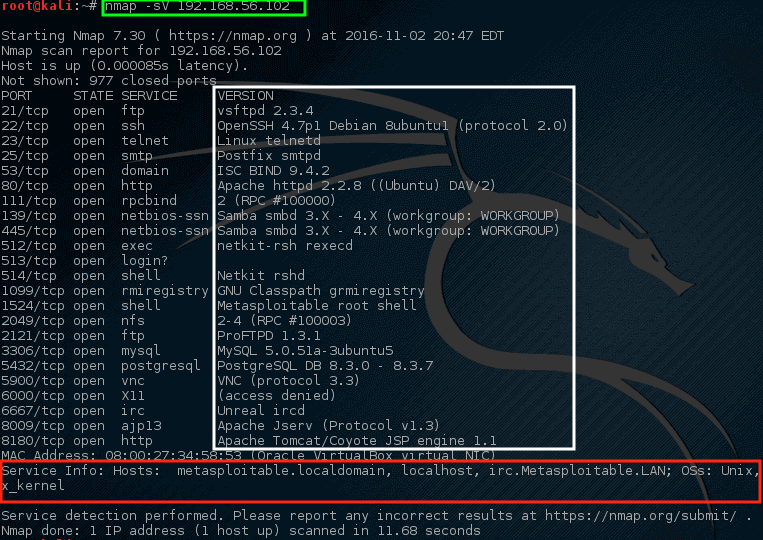


These ports point to a monitoring service on this particular system. When a susceptible system gets issued an IP address, which is why this host has open ports, it can be attacked. Many ports open on a computer is unusual, and the machine should be thoroughly inspected by an authorized administrator. Admins can find the computer that is causing the problem on the network.

**Listening Ports for Services:**

The Nmap program is used to conduct a service scan to see whether any services are currently listening on a certain port. In order to find out what services are running on each open port, Nmap will send out a series of specially crafted packets and interpret any responses.

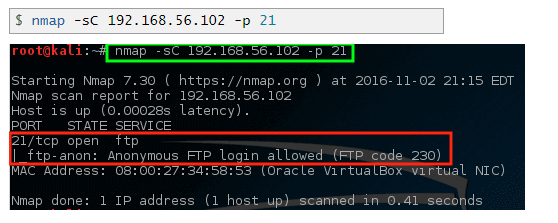




“It works to adopt content about the hostname and the current OS running on the select system. The “vsftpd” version 2.3.4 is performing on this machine,

### Anonymous FTP Logins

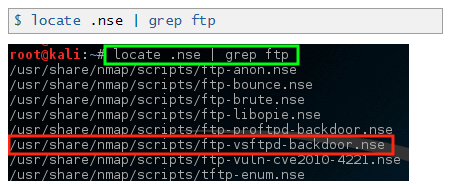
Collectively more information



The above cmd code has establish unidentified FTP sign-in is allowed on this particular server.

### Check Vulnerabilities

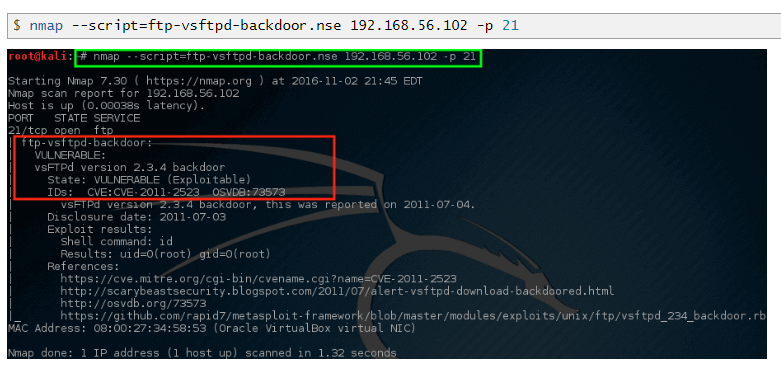
As the declared version of VSftd is old and compromising, so it is quite concerning.



The Nmap scripting engine (NSE) is one of Nmap's most helpful and convertible features. It allows users to write scripts, or "modules," that automate a wide variety of networking tasks. You must learn to use the scripting engine before attempting to execute modules against target machines.

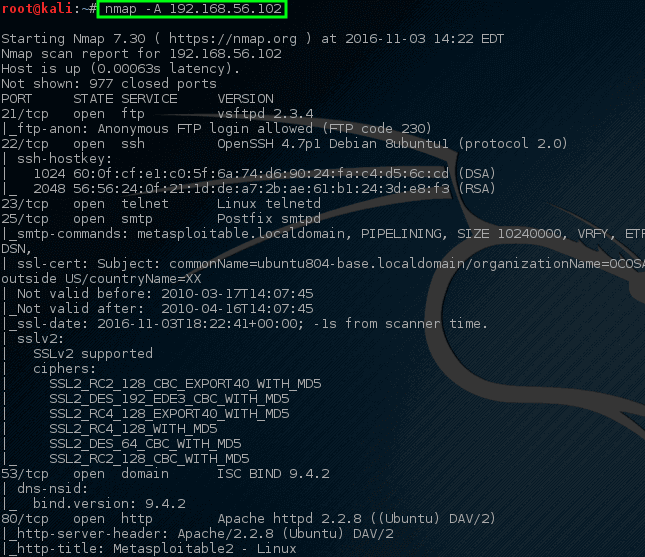


Run the following script:”



Nmap is a quiet and selective tool. For a more thorough scan of a network, use the following command:





## Wireshark Sniffing

**Wireshark is a network protocol analyzer that can be installed on Windows, Linux and Mac. It allows to capture network traffic and analyze it in order to detect various threats.**

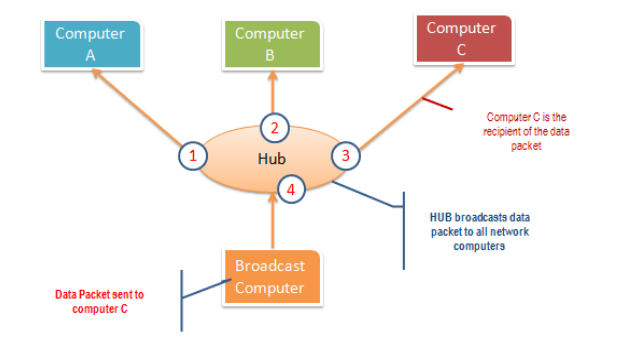
**The latest version of Wireshark at the time of this writing is 2.6.0 which was released on the 11th of February 2019.**

**Wireshark can be downloaded from https://www.wireshark.org/download.html:**

**Installation is straightforward and requires no special permissions, it's enough to download an installer and run it as an administrator.**

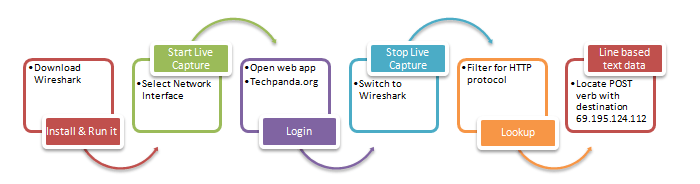
**After installation, you need to select your network interface in order to start sniffing network traffic. To do so, click on "Capture" in the top menus and then on "Options". After that, select your network interface (e.g. WiFi or Ethernet) and click "Start".**

**Here is a diagram of how the hub works in action.**



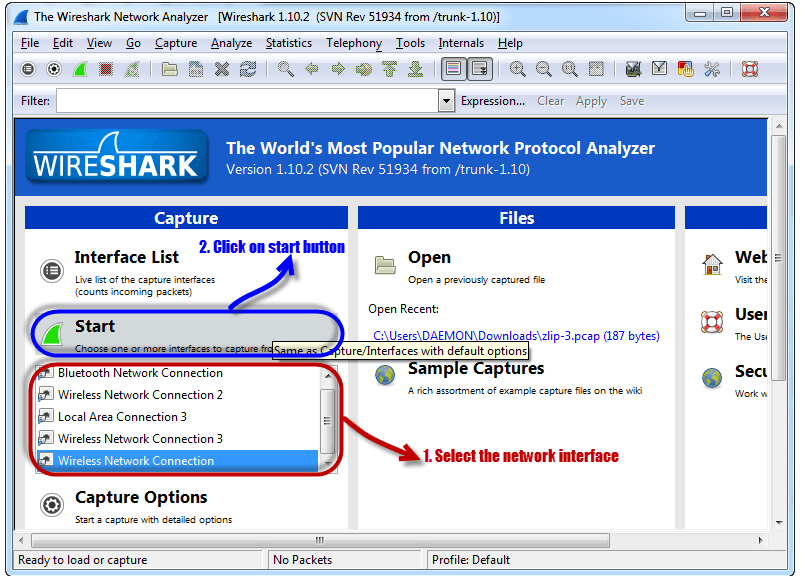
**Due to the mapping of IP and MAC addresses, a computer's IP address will only connect to the physical port whose MAC address is identical. In this way, broadcast messages are sent in a one-to-one fashion only to the intended receiver. At the data link layer (layer 2) and network layer (layer 3), switches are used.**

**The graphic below shows how well the switch works.**



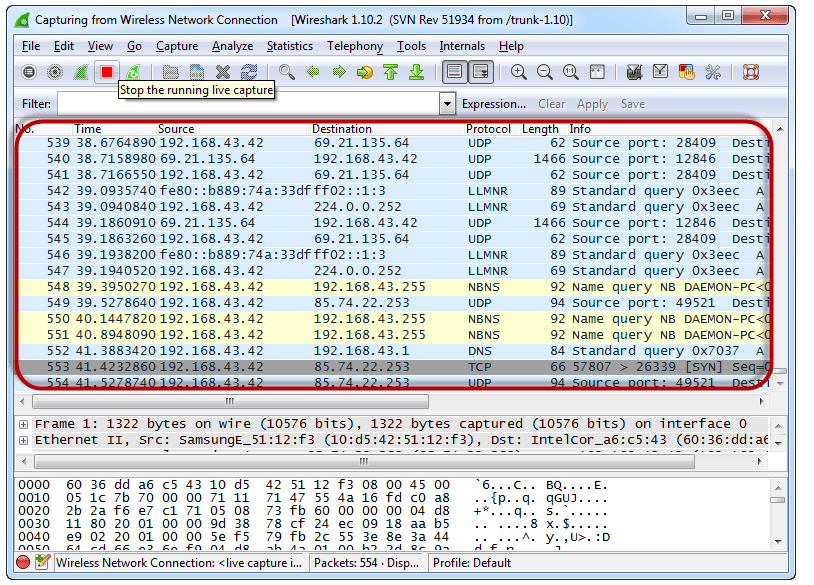
“Download Wireshark from this link [http://www.wireshark.org/download.html](https://www.wireshark.org/download.html)

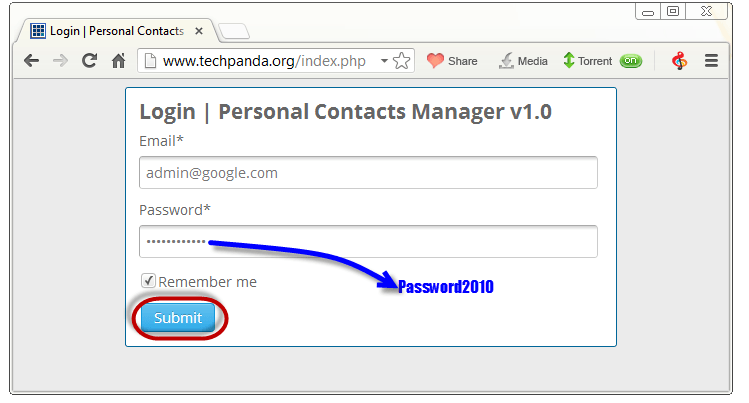
* Open Wireshark
* You will get the following screen”



• To begin, choose the network adapter you want to monitor. 'Note that for this example, we'll be utilizing a wireless connection. In the event that you are connected to a local network, you should pick the LAN interface.

• To begin, press the start button, as seen above.

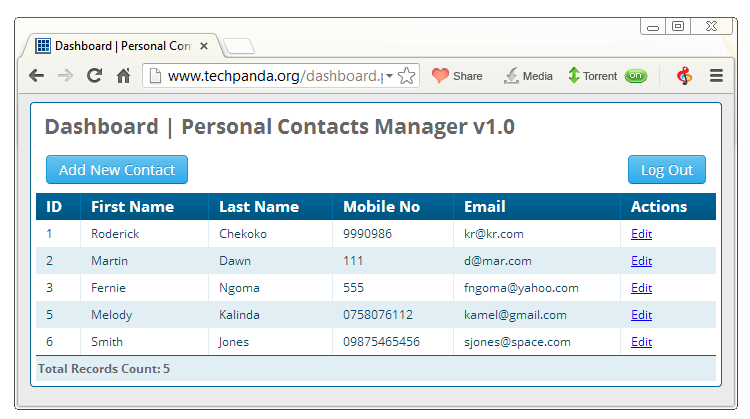




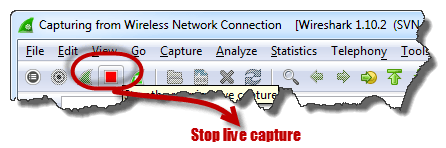
The password is Password2010, The login email is admin@google.com

Click on submit button.

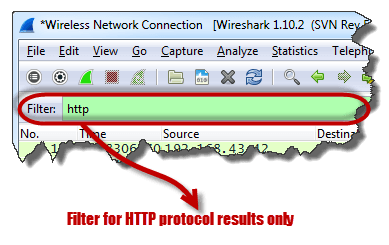
A prosperous logon should give you the following dashboard.



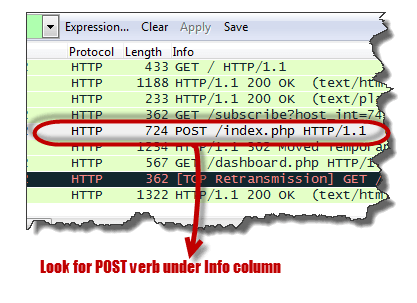
“Go back to Wireshark and stop the live capture



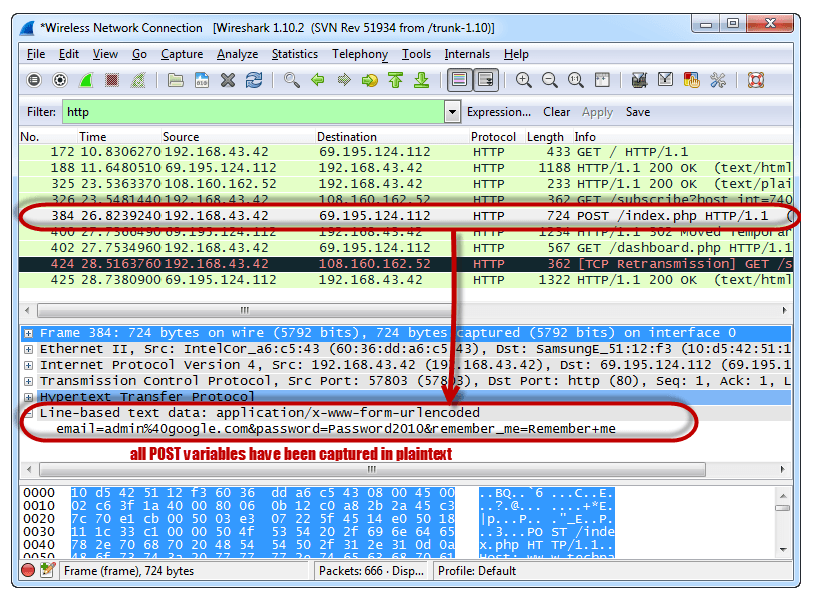
Filter for HTTP protocol results only using the filter textbox



Locate the Info column and look for entries with the HTTP verb POST and click on it”



“Just below the log statements, there is a panel with a extract of represent data. Look for the abstract that says Line-based text data: application/x-www-form-url encoded



You should be able to see the plain text values of all the POST variables submitted to the server via HTTP protocol.”

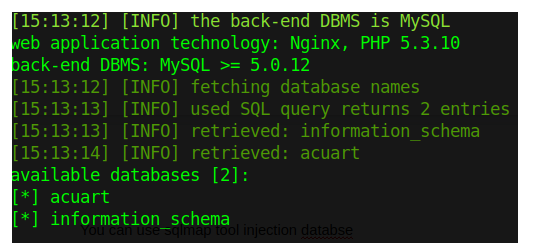
## SQL Injection using SQLMAP

SQLMap, a free and open-source tool for detecting and exploiting SQL injection vulnerabilities, was created. It is for this reason that sqlmap is an application capable of identifying and exploiting SQL injection vulnerabilities. Using a SQL injection attack, an attacker may gain control of a server's database and make changes to its structure.

SQL injection, a hacking technique, may be used to insert SQL commands into a database. Filtering of variables is a common practice among web developers and webmasters alike.

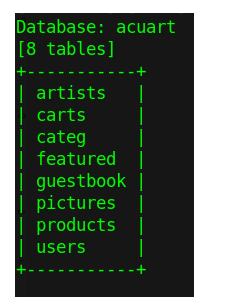
A database is a structured collection of data that can be retrieved by querying a computer or web server.

The first step is to open sqlmap, and then perform the command below.



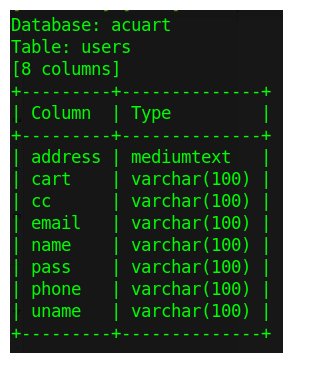
Both finding the database's table names, as well as its database's name, are necessary steps in this process.





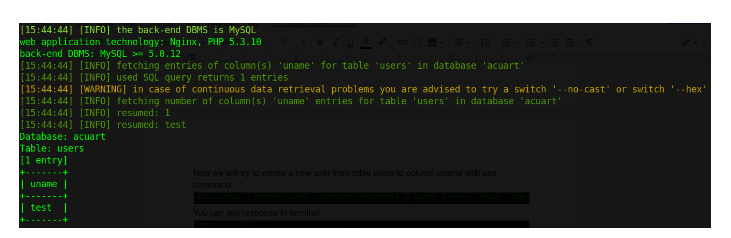
With the table name in hand, we can go on to finding its corresponding field in the custom application database.





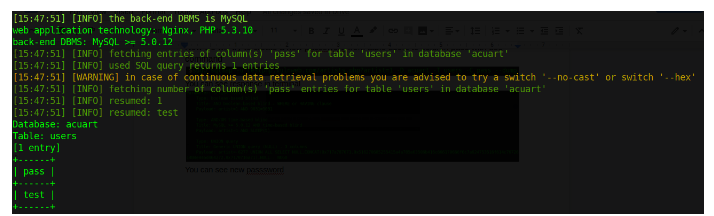
Now, we'll use the following command to find the username stored in the database's acuart table users field uname.





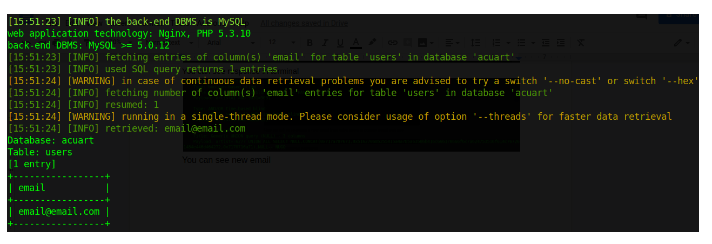
Using the following command, we'll find the username in the data acuart table's users field..





Now, we'll use the following command to find the email address of the user in the data acuart table.





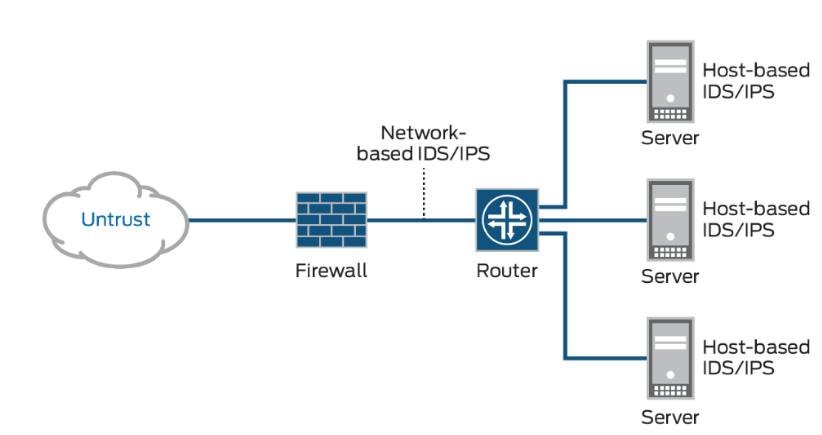
# 

# Design and Implement a web security model

## IDS/IPS

Your network's events are analysed for signals of suspected intrusions, violations, or impending threats to your security regulations, and this is the process of intrusion detection. Intrusion prevention is the practise of first detecting intrusions and then putting a stop to them. There are intrusion detection and prevention solutions available that may be integrated into your network to help you identify and halt any security breaches.

A typical corporate network contains a number of public and private network entry points. Network security while keeping them open to their consumers is a problem. These days, even the strongest security systems are vulnerable to sophisticated assaults, particularly if they are still operating under the notion that networks can be protected by encryption or firewalls. There is no way to stop today's assaults with only those tools.



## Firewall

A firewall is an essential aspect of any security architecture because it removes the guesswork from host-level defences and places them in the hands of your network security device. There are two types of firewalls: those that stop malware and those that block application-layer assaults, and those that include an integrated intrusion prevention system (IPS) that can respond rapidly and smoothly in the event of a network incursion. Invasive or suspect behaviour, such as malware, may be quickly detected and shut off by a network security expert.

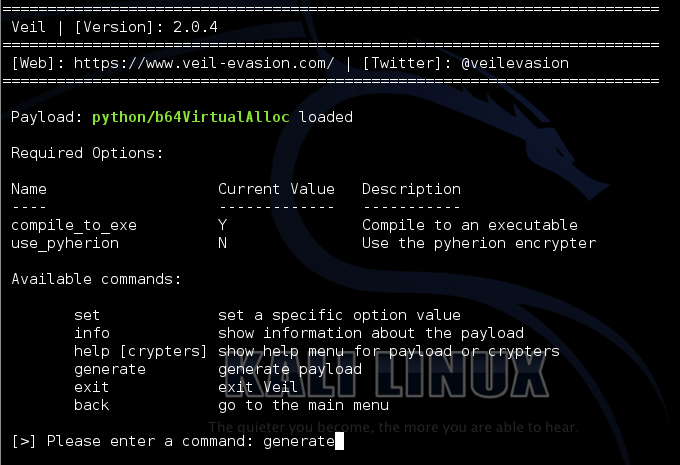
C:\Users\AM ofc manit\Downloads\1111-6.png

## Antivirus

Computer viruses and cyber thieves may be thwarted with the aid of antivirus software. In order to protect your devices, anti-virus software examines the data that travels over the network to your computers. It looks for known risks and keeps track of the activities of all installed apps, alerting the user if anything seems amiss. Viruses are thwarted or removed as fast as feasible using this method.

Antivirus protection is essential because cyberthreats are always developing. Because of this, it is essential that you have anti-virus software installed on your computers and mobile phones to protect against viruses and other dangerous software that may infect your devices without your knowledge. If you already have antivirus software, you could be under the impression that you're protected. Things, on the other hand, may not be as simple as they seem. To keep your computer secure, make sure you're using the latest version of your antivirus programme.

Cyber crooks will attempt to breach your security if there is even a little hole. A smart place to start is to make sure your antivirus software is operating and up to date. As long as identity thieves and fraudsters are always improving their techniques, it's a good idea to use a thorough security solution to safeguard yourself.



# References

* Offensive Security LLC". www.bloomberg.com. Retrieved 2020-03-17.
* Offensive Security Services, LLC". www.buzzfile.com. Retrieved 2020-03-17.
* Penetration Testing with Kali Linux, Black Hat USA 2018". www.blackhat.com. 2018. Retrieved 2020-03-17.
* Speaker Jim O'Gorman, Black Hat USA 2018". www.blackhat.com. 2018. Retrieved 2020-03-17.
* ^ "OSCP cheating allegations a reminder to verify hacking skills when hiring | CSO Online". 2020-03-27. Archived from the original on 2020-03-27. Retrieved 2020-03-28.
* 7 Reasons You Can't Compare the PenTest+ and OSCP – StartaCyberCareer.com". 2020-03-06. Archived from the original on 2020-03-06. Retrieved 2020-03-28.
* Usatenko, Chris (2019-12-12). "Why secure web-based applications with Kali Linux?". Packt Hub. Retrieved 2020-03-20.
* Barr, Joe (13 June 2008). "Test your environment's security with BackTrack". Linux.com. Retrieved 2019-04-10. "BackTrack 4 - Hacking galore". Dedoimedo.com. 2009-05-15. Retrieved 2019-04-10.
* "BackTrack 5 R3 review". LinuxBSDos.com. 2012-08-17. Retrieved 2019-04-10.
* Watson, J.A. (2014-05-28). "Hands-on with Kali Linux 1.0.7". ZDNet.com. Retrieved 2019-04-10.
* "Kali Linux 1.0.7 review". LinuxBSDos.com. 2014-05-30. Retrieved 2019-04-10.
* "Kali Linux review". Dedoimedo.com. 2014-12-15. Retrieved 2019-04-10.
* Watson, J.A. (2016-01-22). "Hands-on with Kali Linux Rolling". ZDNet.com. Retrieved 2019-04-10.
* Smith, Jesse (2016-04-25). "Kali Linux 2016.1". DistroWatch Weekly. No. 658. Retrieved 2019-04-10.
* Kali Linux Penetration Testing Tools". tools.kali.org. Retrieved 2019-04-10
* Kirk, Jeremy (Jul 29, 2014). "Zero-day flaws found in Symantec's Endpoint Protection". PC World. Retrieved 26 September 2015.
* Jump up to:a b "Exclusive: Offensive Security Names New CEO; Former No. 2 at HackerOne, Lynda". Fortune. Retrieved 2020-03-17.
* Ning Wang, Offensive Security LLC: Profile and Biography". Bloomberg.com. Retrieved 2020-03-17.