CTF Preparation Guide

This guide is intended to provide an overview of what a Capture the Flag (CTF) is and provide an overview of some common tools you may want to be familiar with in preparation for a CTF.

Table of Contents

What is a CTF?

A Capture the Flag (CTF) is a competition between security professionals and/or students who are learning about cyber security. The competition is made to help people who are interested in Cyber Security gain knowledge and sharpen the skills they have learned during training.

A CTF is comprised of many challenges. The main goal of challenges within a CTF is to find a flag, which is usually in the format of ‘CTF{flaggoeshere}’. Flags are what everyone is aiming to get by completing challenges, once you obtain a flag, it is submitted into a scoring engine in exchange for points. The amount of points that you receive is based on the difficulty of the challenge completed.

These competitions often require lateral thinking, the name or description of the challenge may give away a hint as to how the player is expected to solve the challenge. Common challenge categories may include, but are not limited to:

- Website Exploitation
- Reverse Engineering
- Digital Forensics
- Incident Response
- Cryptography
- Binary Exploitation

Most challenges give you hints on what you should do to get your flag, such as:

- Maybe you can find an online image decoder?
- NOTE: Flag is not in the usual format
- It would be pretty funny if Jeff forgot to change the default password, right?

Note: Remember, this competition is potentially a hostile environment so make sure your firewall is turned on, you are not exposing services unnecessarily (e.g. SSH on Kali Linux, or file shares and Remote Desktop on Windows). Ensure you are using a long, complex password on your computer and any Virtual Machines (VMs) running. If you are using a Virtual Machine deployed from a template, such as Kali Linux, make sure you change the default ‘root’ password to a long, unique, and complex password. This is a smart move because in a pre-built Kali Linux install, the default ‘root’ password is common knowledge and, if left unchanged, another CTF competitor may gain unauthorised access to your Kali Linux VM.

Practice Makes Perfect

It would be a good idea to start practising before the CTF event so you can gain some knowledge on what everything will feel like, the different difficulties in challenges, and the differences in how direct or indirect hints can be.

picoCTF[1] is an online CTF that will be help you gain some knowledge of what to expect during the competition. picoCTF is free to register and play, however, does require permission from a parent or guardian if you are under 18 years old. The aim of this CTF is to complete the challenges and find the

[1] https://picoctf.com/

flags. Some CTF's, like picoCTF, will provide a virtual computer terminal that you can interact with to complete challenges, access needed directories etc.

Common Tooling

Virtual Machines

Virtual Machines (VMs) allow you to run multiple computers within your physical computer. This is useful during a CTF as it allows you to easily run Kali Linux on your existing computer, giving you many of the tools that may be useful during the CTF. See the section below for information about what Kali Linux is.

How to install

The following instructions apply to Microsoft Windows. A similar process exists for Mac, using a VMWare Fusion trial rather than VMware Player.

1. Download VMware Workstation Player from https://www.vmware.com/au/products/workstation-player/workstation-player-evaluation.html.
2. Once downloaded, install VMware Workstation Player on your computer.
3. VMware Workstation Player is free to use for personal use, no software license is required.

Kali Linux

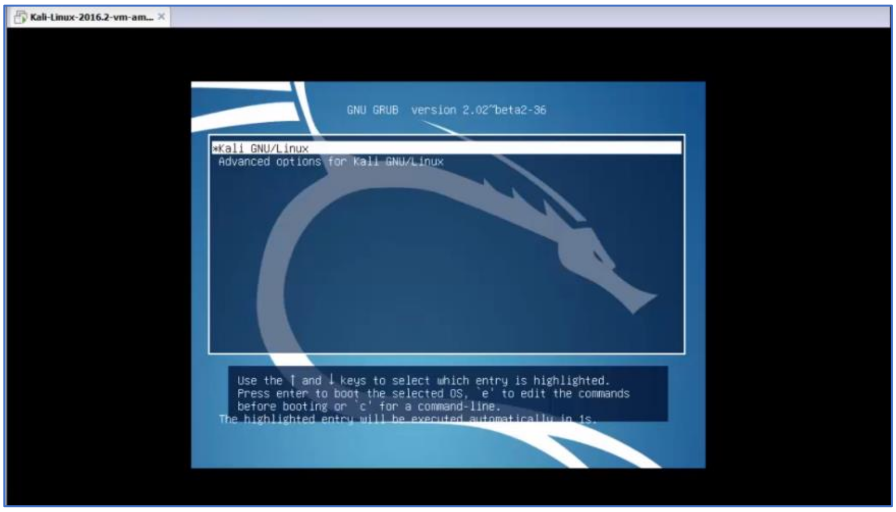
What is it?

Kali Linux is an operating system designed for digital forensics and penetration testing. It is maintained by Offensive Security. This version of Linux contains many tools geared towards different Information security tasks like: Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

Kali Linux comes with Wireshark, Burp Suite Community Edition, and Firefox already pre-installed on it, so you are ready to go.

How to install it?

1. Browse to https://www.offensive-security.com/kali-Linux-vm-vmware-virtualbox-image-download/7/.
2. Locate the Kali Linux VMware Images section and choose the either the 32-bit or 64-bit and wait for it to download. If you only have 2 – 4 GB of RAM you would be better off getting the 32-bit version, if you have more than 4gb of RAM available, the 64 bit version will be better for you.
3. The downloaded file is a 7-zip file, you will need to install that from https://www.7-zip.org/download.html.
4. Once the file has downloaded, extract the 7-zip file. There should now be a folder called Kali-Linux-2019.1-vm-amd64.
5. Launch VMware Workstation Player and choose Player, File, Open. Locate the Kali Linux VMX file and click Open.
6. Press Power on this virtual machine. A message may pop up click "I copied it".
7. The below boot screen should appear, simply waiting a few seconds will allow Kali Linux to boot.



```
GNU GRUB  version 2.02~beta2-36

*Kali GNU/Linux
 Advanced options for Kali GNU/Linux

   Use the ↑ and ↓ keys to select which entry is highlighted.
   Press enter to boot the selected OS, `e' to edit the commands
   before booting or `c' for a command-line.
The highlighted entry will be executed automatically in 1s.
```

8. After it loads you will be asked for a username and password, the default username is ‘root’, and the password is ‘toor’.
9. Because the default Kali password is public, the first thing you want to do after logging in is change your password. Open the terminal and type in ‘passwd’. You will then be prompted to create a new one. Ensure you enter a unique and complex password.
10. You now have Kali Linux set up on your Virtual Machine.

Burp Suite

What is it?

Burp Suite is graphical tool, specifically a web interception proxy, used to test web application security. A few useful modules within Burp Suite include:

- **Proxy:** A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. Burp Suite functions as an HTTP proxy server, with all HTTP/S traffic from your browser passing through it. To do any kind of testing with Burp, you need to configure your browser to work with it.
- **Proxy – HTTP History:** HTTP History maintains a full record of all network traffic that has passed through the proxy. You can filter this information to help manage it and use the proxy history to drive your testing workflow. The proxy history is always updated even when you have intercept turned off, allowing you to browse without interruption while still monitoring all details about application traffic.
- **Proxy - Intercept:** You can intercept all requests from your browser, and you must approve any requests for them to go through. Intercept allows you to manipulate requests as they are being sent.
- **Intruder:** You can use Intruder, which allows the user to launch attacks on a website. You can do ‘brute force’ attacks through the Burp Suite Community Edition but it is extremely slow so you may want to look for another product, such as Hydra. Hydra is already installed on Kali otherwise, ‘sudo apt install hydra’ would install it on other Linux systems.
- **Repeater:** You can use Repeater to manually manipulate and repeat individual HTTP requests and analyse the application’s response.
- **Decoder:** Is a simple tool for encoding and decoding data into various encoded and hashed forms. It is also able to encode and decode URL, HTML, Base64 strings to text, ASCII text,

Hex, Octal, Binary, and Gzip. You may also use CyberChef[2] which is another great tool to use if you encounter code that needs decoding, Burp Suite is good enough to use if you happen to come across Base64 and need to quickly decode it.

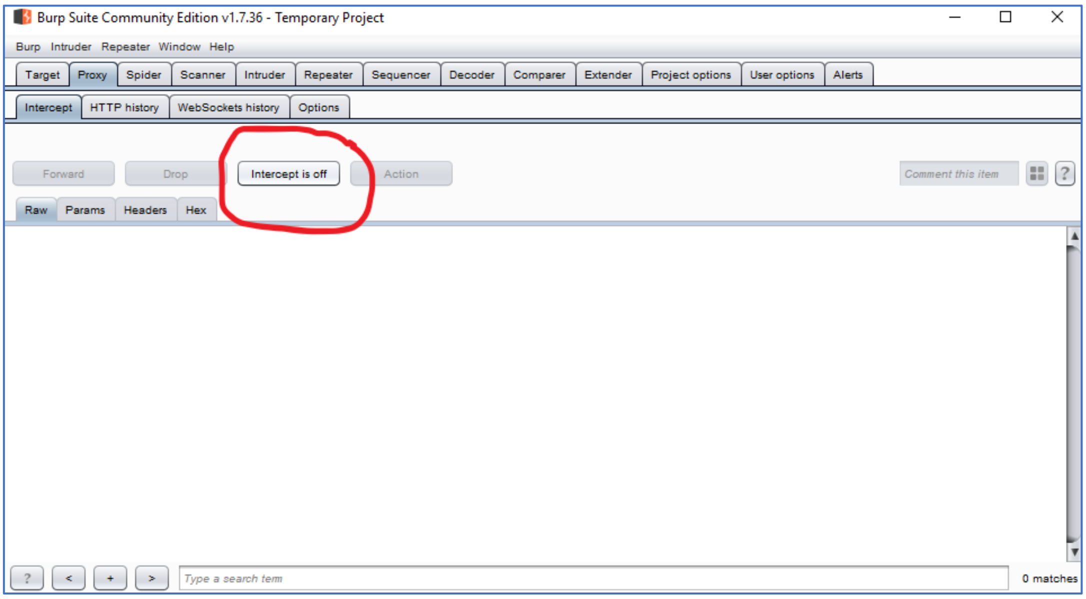
How do I set up Burp Suite?

Burp Suite Community Edition is already installed in Kali Linux. Below are details on how to configure Burp Suite:

1. Burp Suite Community Edition is already installed in Kali Linux. If you do need to install it, you may download it from https://portswigger.net/burp/communitydownload.
2. If not already installed, download and install Mozilla Firefox from https://www.mozilla.org/en-US/firefox/new/.
3. Open Burp Suite and click "next" and then "start burp" on the prompts.
4. Open Firefox click the three line button in the top right-hand corner, and click options. Where it says 'Find in Options' type Proxy and click on settings when in pops up.
5. Select Manual proxy configuration and type 127.0.0.1 in the bar below it, next to it where it asks for a Port, put 8080, and make sure the "use this proxy server for all protocols" box is checked.
6. Delete anything in the "no proxy for" field.
7. Now click okay.
8. Now you need to install the Burp Suite Certificate.
9. In the search bar in Firefox, put http://127.0.0.1:8080/.
10. At the top left corner of the webpage you will see CA Certificate, click that. You will be asked whether you want to open the file or save the file, choose to save, and make a note of where you are saving it to.
11. Find the folder from where you saved it, open it, and then click install. Click current user click next, leave the circle that says "Automatically select the certificate based on the type of certificate" checked and click next. Now click finish.
12. Now go back to options in Firefox and type 'certificates' instead of 'proxy'. Click on view certificates.
13. Make sure you are in the Authorities tab and scroll down until you see import. Click on the certificate from wherever you saved it to and open it. In the dialogue box that pops up, check the box "Trust this CA to identify web sites" and click okay.
14. If you have done everything correctly you should now be able to go into Burp Suite, click the Proxy tab, then click the HTTP History tab and see all web traffic browsed within Firefox since enabling the Proxy. If it doesn't work straight away, try restarting your virtual machine.

Note: Remember to turn intercept off if you don't want to have to authorise everything you're doing on Firefox. The Intercept button appears in the Intercept tab, as shown in the below screenshot.

[2] https://gchq.github.io/CyberChef/

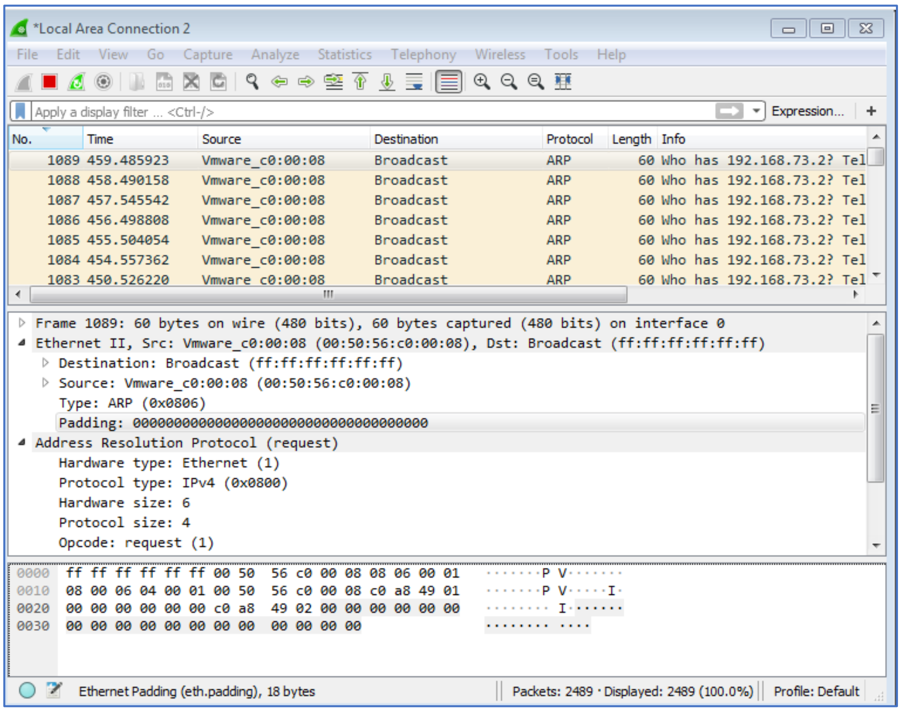

Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is off
Action
Comment this item
Raw Params Headers Hex
Type a search term
0 matches

Wireshark

What is it?

Wireshark is a free and open-source packet analyser. It lets you see what's happening on your network at a microscopic level. Wireshark is compatible with Windows, Linux, and MacOS. If you have Kali Linux installed it already has Wireshark preinstalled on it, so you can start using it as soon as Kali Linux is installed. Otherwise, Wireshark can be downloaded from https://www.wireshark.org/download.html.

In addition to analysing live network traffic, Wireshark can save and open 'PCAP' files. This allows you to review events that have previously occurred, useful for Digital Forensics (and Incident Response CTF challenges). The screenshot below demonstrates Wireshark displaying Address Resolution Protocol (ARP) traffic, without any applied filters.


*Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time        Source            Destination  Protocol  Length Info
 1089 459.485923  Vmware_c0:00:08   Broadcast    ARP          60 Who has 192.168.73.2? Tel
 1088 458.490158  Vmware_c0:00:08   Broadcast    ARP          60 Who has 192.168.73.2? Tel
 1087 457.545542  Vmware_c0:00:08   Broadcast    ARP          60 Who has 192.168.73.2? Tel
 1086 456.498808  Vmware_c0:00:08   Broadcast    ARP          60 Who has 192.168.73.2? Tel
 1085 455.504054  Vmware_c0:00:08   Broadcast    ARP          60 Who has 192.168.73.2? Tel
 1084 454.557362  Vmware_c0:00:08   Broadcast    ARP          60 Who has 192.168.73.2? Tel
 1083 450.526220  Vmware_c0:00:08   Broadcast    ARP          60 Who has 192.168.73.2? Tel
```

```
▷ Frame 1089: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
◢ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▷ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▷ Source: Vmware_c0:00:08 (00:50:56:c0:00:08)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
◢ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
```

```
0000  ff ff ff ff ff ff 00 50  56 c0 00 08 08 06 00 01   ·······P V·······
0010  08 00 06 04 00 01 00 50  56 c0 00 08 c0 a8 49 01   ·······P V·····I·
0020  00 00 00 00 00 00 c0 a8  49 02 00 00 00 00 00 00   ········ I·······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Ethernet Padding (eth.padding), 18 bytes | Packets: 2489 · Displayed: 2489 (100.0%) | Profile: Default

Nmap

What is it?

Nmap is a free and open-source network scanner that is used to discover hosts and services on a computer network by sending packets and analysing the responses. It runs on Linux, Windows and MacOS, and is already installed on Kali.

Nmap is primarily used for:

- Discovering network components (e.g. workstations and servers)
- Determining open ports and services running on a host
- Determining the Operating System running on a host

Nmap should already be installed on Kali but if it isn't open the terminal and type in 'sudo apt install nmap' and it should download and install.

Nmap examples

In the Linux terminal you can type in 'nmap -v (ip address)' and it will bring up information on ports that are related to that address. To scan all 65535 TCP ports, add the flag '-p- '. The example below would scan for all TCP ports opened on the IP Address 127.0.0.1 and run probes for further information regarding the services identified:

```
nmap -sV -A -sC -p- 127.0.0.1
```

There are many different parameters to use:

- Scan using IP address – nmap 192.168.1.10

- Scan using '-v' option – nmap -v (ip address) – provides more verbose information during the scan
- Scan an IP address range – nmap 192.168.1.1-10
- Scan a Network IP Range for devices - 'nmap -sP 192.168.1.0/24' - this would scan the whole CIDR /24 (which is 255 hosts).

Note: Ensure you have permission prior to scanning an IP address or ranges of IP addresses prior to running nmap against target.

Linux Commands

The Linux terminal is very useful during a CTF. Some common commands are listed in the table below.

Command	Description and Example
ls	**List:** The ls command shows all the main directories filed under a file system.
cd	**Change Directory:** Allows the user to change between file directories. e.g. 'cd Documents/'
mv	**Move:** Allows the user to move a file or folder to another directory, e.g. mv (current file location)/(file name) (new file location)/ Examples include: • Typing 'mv Documents/test1 Downloads/' into the terminal would move the test1 file into the Downloads folder • You can also use this command to rename a file or folder, e.g. mv oldfilename newfilename
cat	**Concatenate:** Despite its name the cat command is most commonly used to read the contents of a file and print them into the terminal, e.g. cat notes.txt
man	**Manual:** The 'man' command is used to display information of the inputted command e.g. 'man mv' you will see information on the operation mv, you also see command flags and what they do like; -n, -S, -t and many more.
mkdir	**Make Directory:** Allows the user to create a new directory e.g. mkdir (name the new directory).
rm	**Remove File (Delete):** This command allows the user to delete created files, it is like 'rmdir' which removes directories. e.g. rm (name of file with the format at the end - .txt/.doc/.docx)
rmdir	**Remove Directory:** Allows the user to remove a directory e.g. rmdir (name of directory to be removed), this will not work if the directory has files in it.

Command	Description and Example
touch	**Create a File:** This command is like mkdir, the difference is that mkdir creates directories, whereas touch makes files. You can put whatever extension you would like the file to have but typically you would use touch to create a .txt file e.g. touch notes.txt
clear	**Clear:** This command is used to clear your terminal screen.
history	**History:** This command shows you all previous commands that have been used in the current terminal.
< or >	**Redirection Operators:** These two symbols are operators for Linux, they basically allow you to input a file to a command, or output a command to a file, respectively. e.g. 'nc ip.address.of.server 9090 < python testscript.py' the server will connect to the port 9090 and then run the python script against it.
|	**Pipe:** A pipe is a form of redirection that is used to send the output of one program to another program for further processing. E.g. cat (file name) | grep (string). For example, If I had a file called fruits.txt and it contained; apple, melon, banana, rockmelon, watermelon, and pear, and typed the 'cat fruits.txt | grep melon' into the terminal, the system would then search the file fruits for the word melon and show us only words containing melon, so I would only be shown: melon, rockmelon, and watermelon.
nc	**Netcat:** A utility that reads and writes data across network connections, using the TCP protocol by default. It is a tool that can be used directly or driven by other programs and scripts, as demonstrated earlier with 'nc ip.address.of.server 9090 < python testscript.py'.
grep	**Grep:** Searches for patterns in a file or command output. Examples include: • Typing 'cat fruits.txt | grep melon' into the terminal, the system would then search the file fruits for the word melon and show us only words containing melon, so I would only be shown (e.g. rockmelon, watermelon, and melon). • Typing 'cat fruits.txt | grep -v melon' into the terminal, will then bring up everything in the fruits document that does not contain apple.

Appendix I: Damn Vulnerable Web Application

What is it?

The Damn Vulnerable Web Application (DVWA) is an application that intentionally includes a range of common web application vulnerabilities. DVWA allows people to practise their web application hacking skills in a safe and legal manner. There are varying levels of difficulty, and walkthroughs online if you really get stuck.

The DVWA provides a platform to practice the following attacks:

- Brute Force
- Command Injection

- CSRF
- File Inclusion
- File Uploads
- Insecure CAPTCHA
- SQL injection
- SQL injection (blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript

How to install

XAMPP

Xampp is the web server which will host the DVWA web application. It is recommended to install XAMPP within a Windows VM on your computer.

Note: DVWA is vulnerable by design. If installed directly on your normal computer, an attacker on your network may compromise the DVWA and gain unauthorised access to your computer. XAMPP and DVWA should preferably be installed on a VM and the network adapter set to Network Address Translation (NAT) mode to ensure you are not unintentionally exposing a vulnerable web application on your computer.

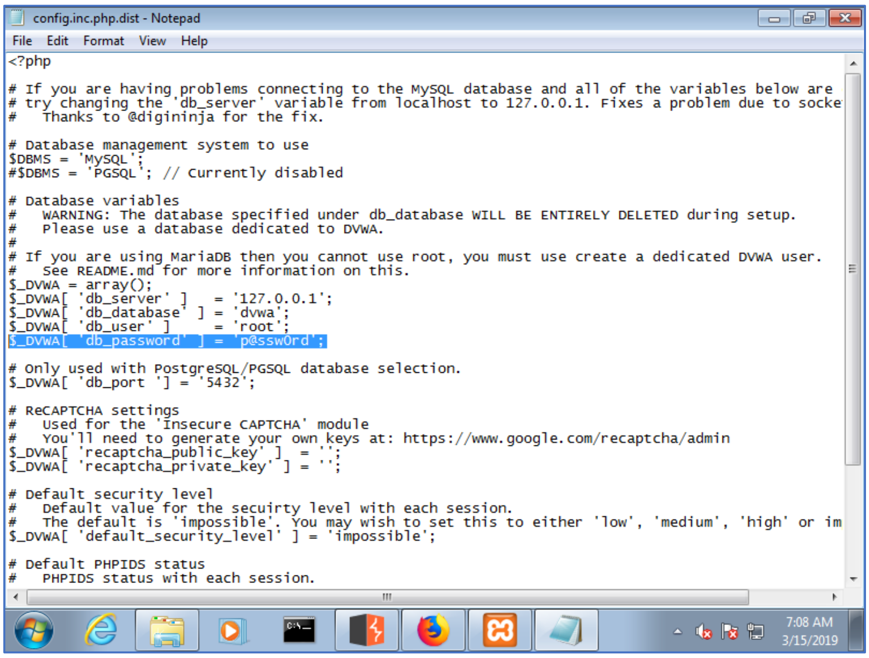
1. First you want to download XAMPP from Apache friends, with the following link https://www.apachefriends.org/index.html.
2. Double click the file to run the installer and click the ok button on the warning.
3. Click next, it is recommended to leave the default options and click next.
4. Use the default install location or choose your own, click next.
5. Uncheck the box that says, 'Learn more about Bitnami for XAMPP'.
6. Click allow access to allow the app through your firewall (if applicable).
7. Click finish, then choose your language and click the save button.
8. Open XAMPP, look for Apache and MySQL, making sure that they both say stop on the right, click the red cross on the left of both and click Yes when prompted.
9. You can now run Apache and MySQL.

DVWA

As DVWA is a web application, it needs to be installed on the same computer or VM that you installed XAMPP.

1. Go to http://www.dvwa.co.uk/ and scroll down until you see download.
2. Check the save file bubble and click okay.
3. Open Downloads, you should see a zip file called DVWA-master. Copy that file.
4. Go to C:\xampp\htdocs and paste the folder here.
5. Right click the zipped folder and click extract all, then click next. Close the file window that pops up.
6. Back in htdocs file, delete the zipped folder, and rename the unzipped folder to dvwa.

7. Open the dvwa\DVWA-master\config\config.inc.php.dist open this document with notepad and look for where it has ‘p@ssw0rd’ and delete the password so that there is nothing between the quotation marks. Save your changes and close the window.



```
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to socke
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';

# Only used with PostgreSQL/PGSQL database selection.
$_DVWA[ 'db_port '] = '5432';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
#   Default value for the secuirty level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or im
$_DVWA[ 'default_security_level' ] = 'impossible';

# Default PHPIDS status
#   PHPIDS status with each session.
```

8. Now copy the config.inc.php.dist document and paste it in the same location. Right click on the copy and rename it to config.inc.php
9. Now open a web browser and type in 127.0.0.1/dvwa/, you should see your folder pop up, click on it and you will be taken to the login page: user: admin password: password.
10. Scroll down to the bottom of the page and click on Create/Reset Database.
11. When the page reloads, wait a little bit and you will be redirected to the login page.
12. Login with the same details.
13. Now when the page loads you will see more information and things like Brute Force, CSRF, SQL Injection etc.
14. Scroll to the bottom of the page and click on DVWA security, now choose the difficulty you want to start with, if you’re a beginner it is recommended that you start at low and work your way up.