



Course: Applied Computer Security (A7010E)

Name: Mubashir Ali

Department:

Major: Master in Information Security

Solution of Assignment 4

**Question 1: Write a two-page essay on one of the following topics:**

- Malware classification
- Malware countermeasures

**Topic: Malware classification**

**Outline:**

1. Introduction
2. History of Malware
3. How Malware spreads?
4. Types of Malware
  - 4.1. Viruses
  - 4.2. Trojan horses
  - 4.3. Worms
  - 4.4. Spyware
  - 4.5. Zombie
  - 4.6. Phishing
  - 4.7. Spam
  - 4.8. Adware
  - 4.9. Ransomware
5. Mitigation measures
6. Conclusion

The rapid increase in population has great implications. One of the greatest implications of the population explosion is the increase in the use of internet. The internet has made communication easier and quicker. With the evolution of internet and the emergence of new technologies in computing, the risks associated with the use of internet have also increased. The rise of internet banking, social media, Ecommerce, and several other technologies has also exposed the vulnerabilities in the internet. Several flaws have been identified in the internet. One of the most common vulnerabilities, is the Malware. Malware short for ‘malicious software’ is a program that is used or developed for the purpose of gaining access to sensitive information of one’s computer, to disrupt computer operations, and to gain private information of any critical system. It can be in any of the forms like code, script, malware software, or active content.

The history of malware goes back when the first malware named ‘Creeper worm’ was developed by Bob Thomas at BBN technologies in 1970s. It was a self-replicating program designed to test how a program can move from one computer to another. In 1980s, another malware type virus named ‘Elk Cloner’. It was also a self-replicating program that affects personal computers. In the 2000s various types of malware viruses have been detected like ‘I love you worm’, ‘SQL slammer worm’, and ‘conficker worm’, etc. In 2011 a new type of malware was identified named as ‘Zeus Trojan’. It was specifically designed to steal the banking information. This malware got great success in its initial years. The latest effective malware was ‘WannaCry Ransomware’ identified in 2017. It was designed to exploit vulnerability that was identified by the National Security Agency (USA). This malware caused drastic damage to computers as it demands the people to pay a ‘ransom amount’ in order to get rid of it. The scope of this malware included many countries like China, Russia, the UK and the USA. It had affected 150 countries including their critical infrastructures like hospitals, banks, and telecommunication, etc.

The spreading of malware in any computer may be through the internet, or from a local CD or DVD, or infected USB. When we download or install an infected software, it enters in our system and starts affecting its targeted files. Some malwares may be executed before their activation, some may start their execution instantly. The malwares can also attack networks by breaking the network security infrastructure. The main targets of malware are operating system, data disks and in some cases it affects the entire network. Almost all malwares are self-replicating programs. In the following section main types of malwares are discussed.

One of the most common malware types, is the virus. The virus is a simple self-replicating program. All viruses are man-made. It can be in the form of a script or code. They can cause major damage to system files, hard disks, operating systems, and web browsers. Examples of computer viruses are macro virus, logic bomb virus, resident virus, etc.

The other type is the Trojan Horse. Its appearance looks like an important program that has important functionalities. But in reality it can cause severe damage to computer security. It is used to capture the login and password credentials. Trojan Horse must be sent by someone or carried by another program or maybe in the form of joke program. It is not a self-replicating program. Examples of Trojan Horse are Remote access Trojans (RATs), Backdoor Trojans (backdoors), IRC Trojans (IRCbots), and Keylogging Trojan

Worms are another type of malware. It is a self-replicating program and uses a network to send infected copies of itself to other computers on the network. The entire system may be collapsed due to worms. Types of worms are internet worms, email worms, file-sharing worms, etc.

Spyware are the malwares that are used for surveillance of computer user. It is installed in the system without the knowledge of the user and it is typically difficult to detect. Spywares usually steal login and password credentials. Examples of spyware are browser hijack, adware, keyboard loggers and much more.

Another type of malware is the zombie. These malware get the control of one's computer and use that computer to attack other computers to perform criminal activities. Examples are Man-in-the-middle, Man-in-the-browser, backdoor hijacking. Phishing is a malicious message that tries to steal login and password credentials while spam is an email that a person did not request. Phishing may be a code while spam is in the form of email.

Adware is basically used for advertisement and for spreading viruses, Trojans, etc. It is in the form of pop-up ads on the websites. On the other hand, ransomware is a malware that is typically in the form of a script or program that holds the control of computer and demands a certain amount as ransom.

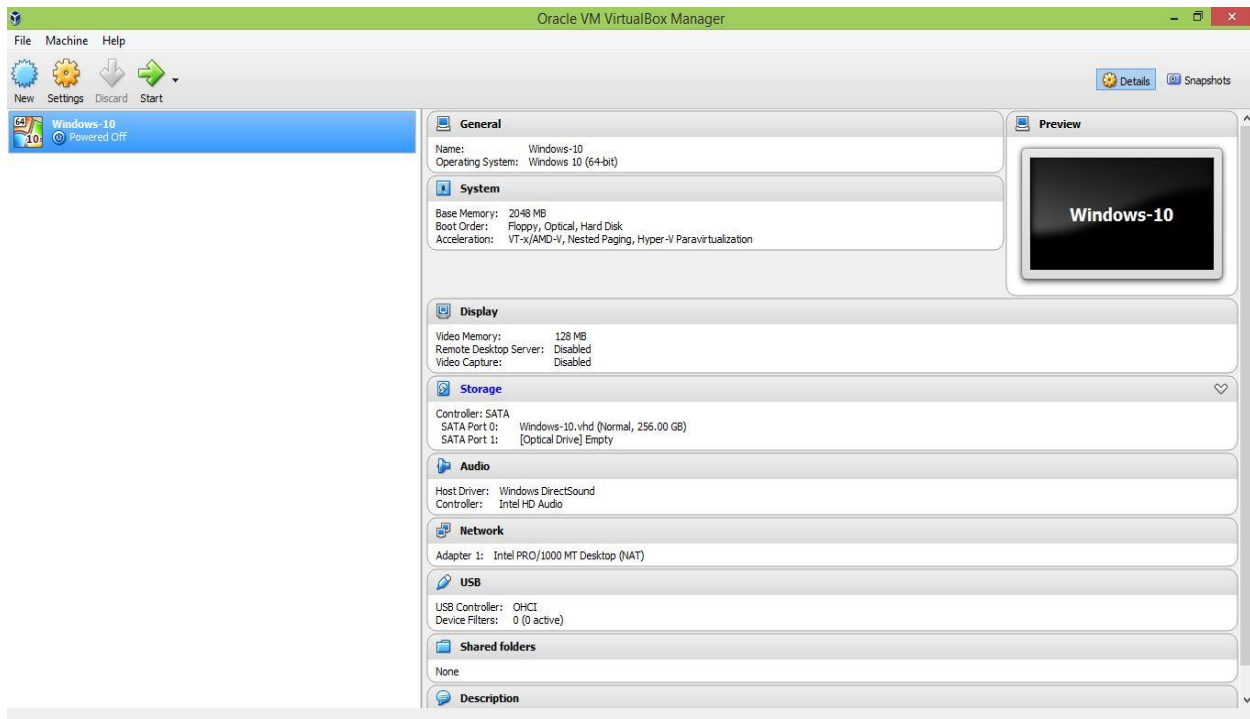
After discussing different types of malwares, there are some mitigation measures that must be adopted for securing computer. For instance, use of antivirus, anti-spyware and anti-spam software, enable firewall in windows. To conclude, for secure communication and to avoid data loss, computers should be protected. Otherwise the implications of less secure system are huge including financial, human resource, and computer etc.

## Question 2: Lab assignment

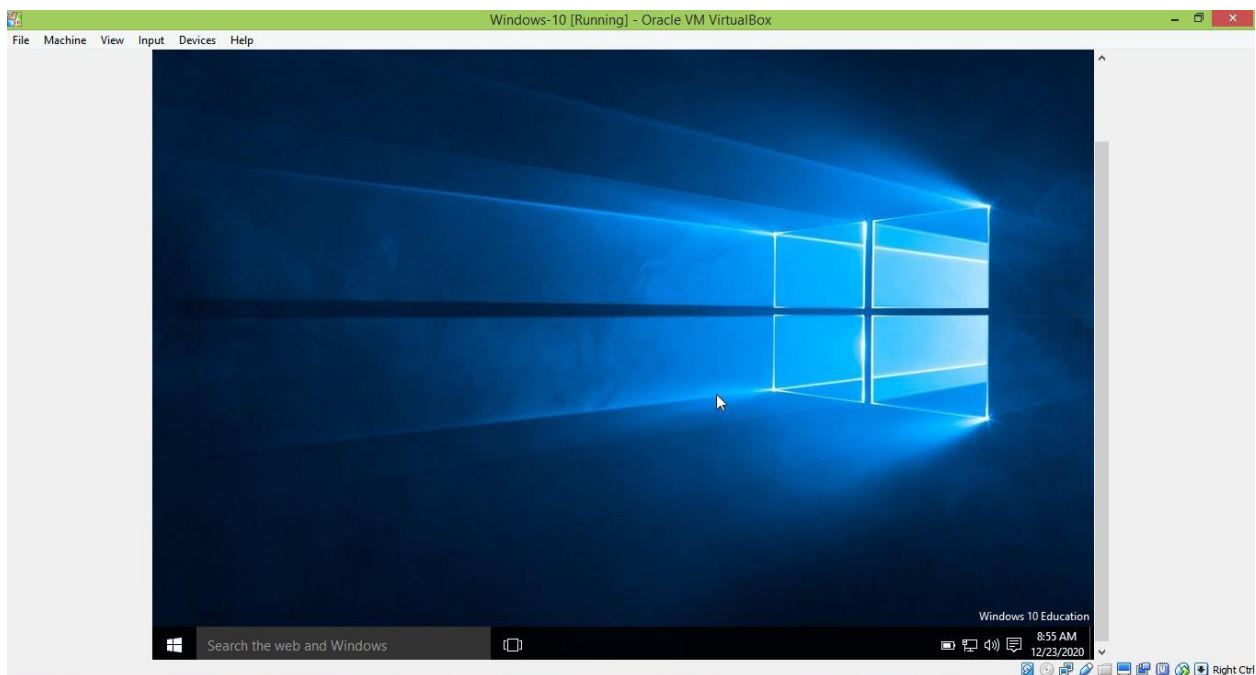
### PART ONE

#### Virtual Box and Windows 10 installation:

**Step 1:** In this step a new virtual machine is created. Here we are using Windows 10

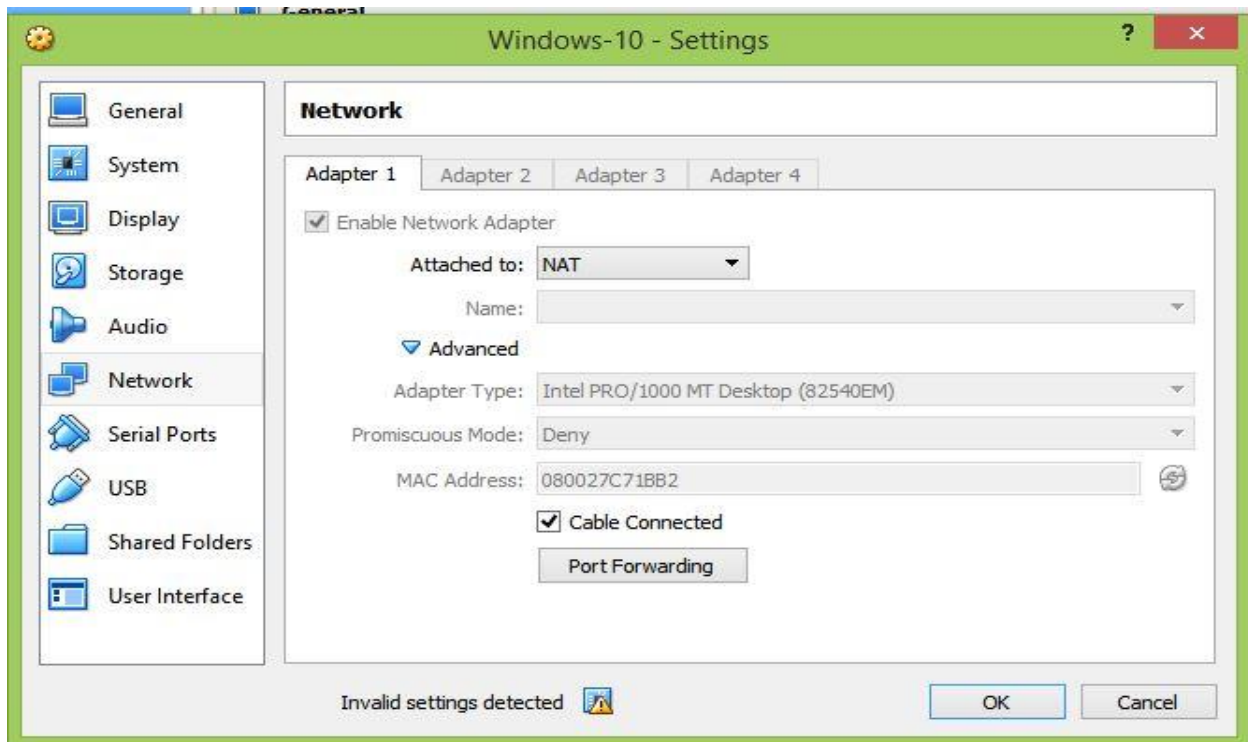


**Step 2:** In this step successful installation of Windows 10 is demonstrated as below.

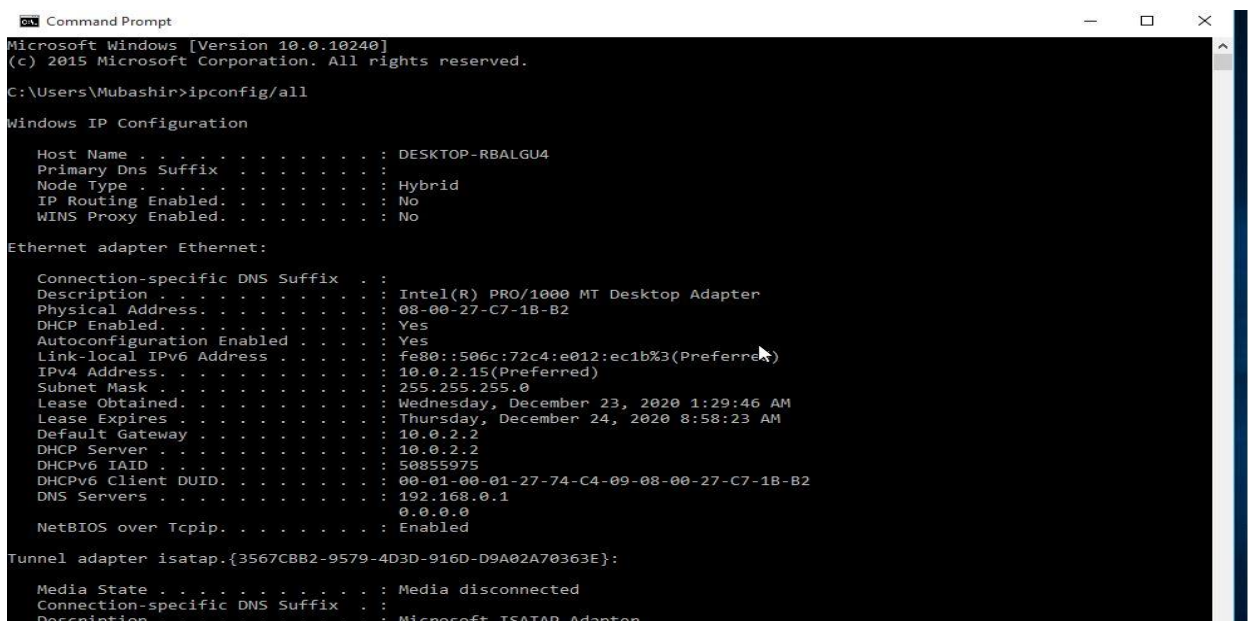


**Step 3:** In this step, we will change the settings of the NAT network adapter so that we can use the internet. The internet access is necessary for downloading the required software. The demonstration of this is shown in the figure below.

**Note:** The Virtual machine must be powered off in order for the changes to take place.

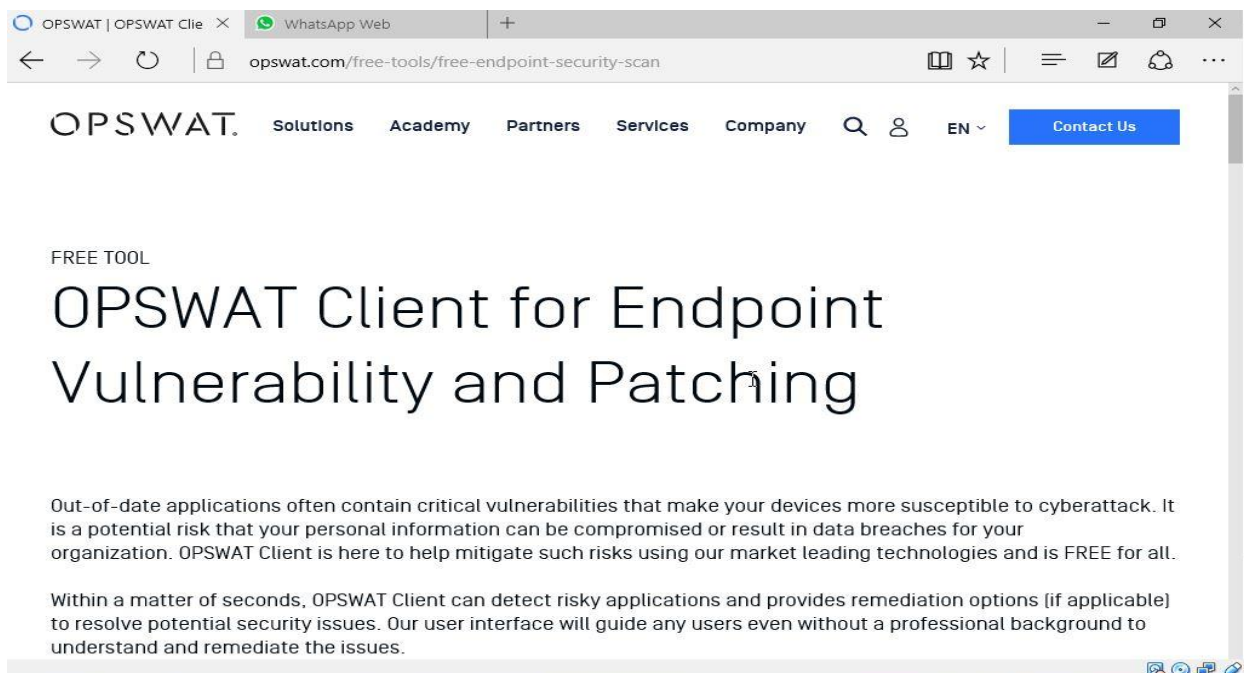


**Step 4:** Now start the virtual machine and test the connectivity by typing 'ipconfig/all' command in the command prompt as shown in the figure.

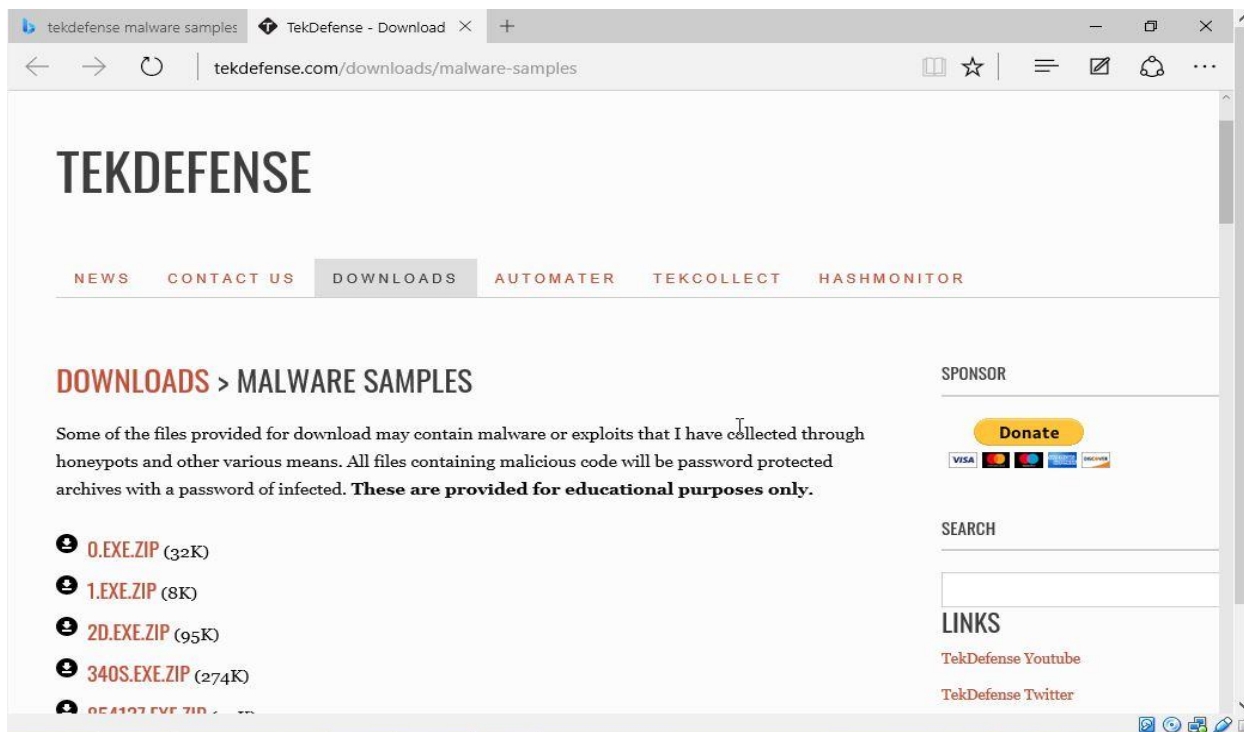


## Part 2: Downloading Malware tools and samples to test

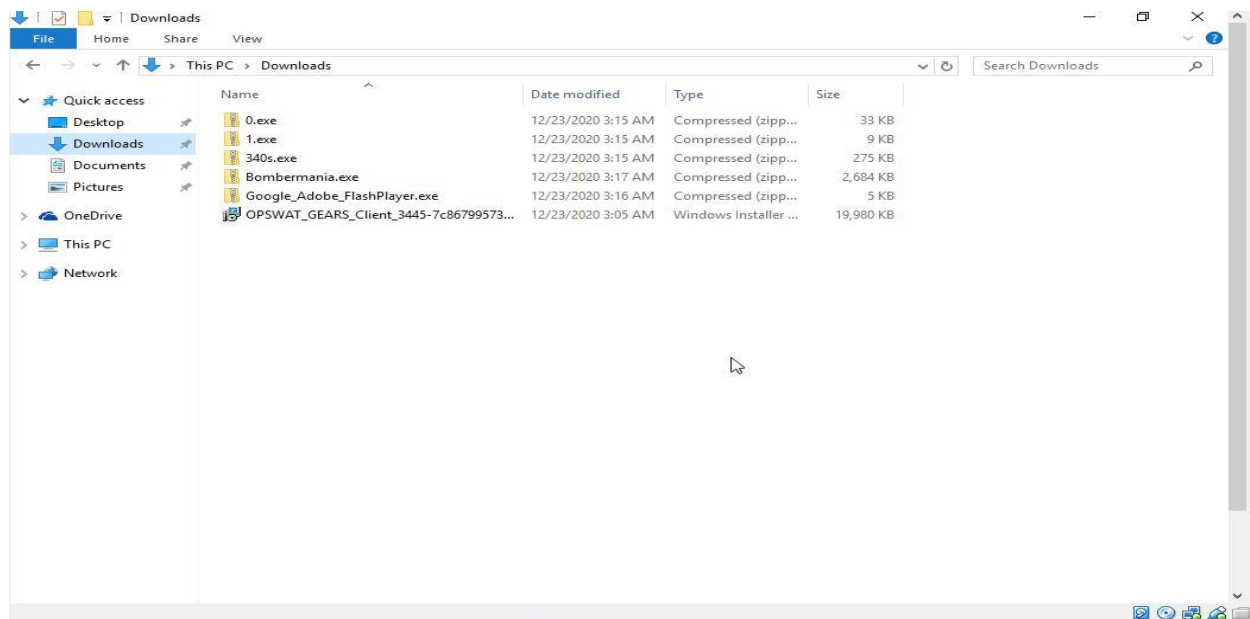
**Step 1:** Browse to the following address <https://www.opswat.com/free-tools/free-malwareanalysis-tool> to download the MetaDefender Client Malware analysis tool.



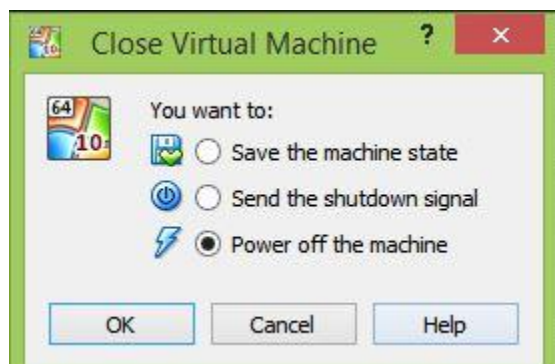
**Step 2:** Browse to the website <http://www.tekdefense.com/downloads/malware-samples/> to download malware samples for testing



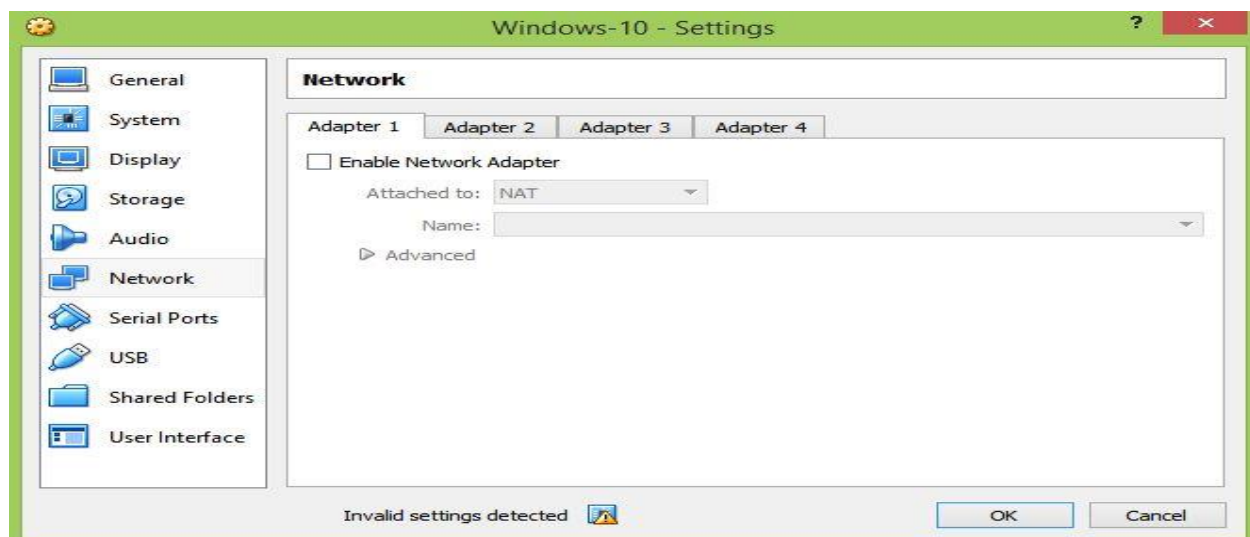
### Step 3: Downloaded samples



### Step 4: Machine will be powered off to disconnect it from the network

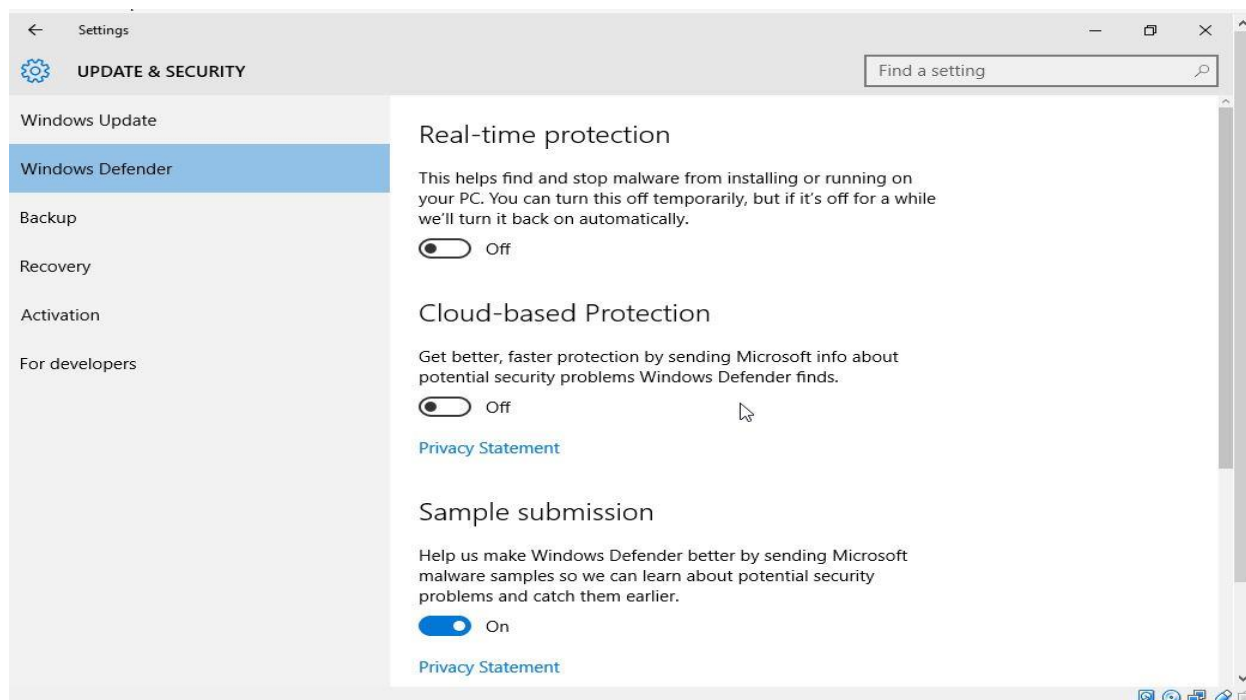


### Step 5: Unchecking the Ethernet cable adapter

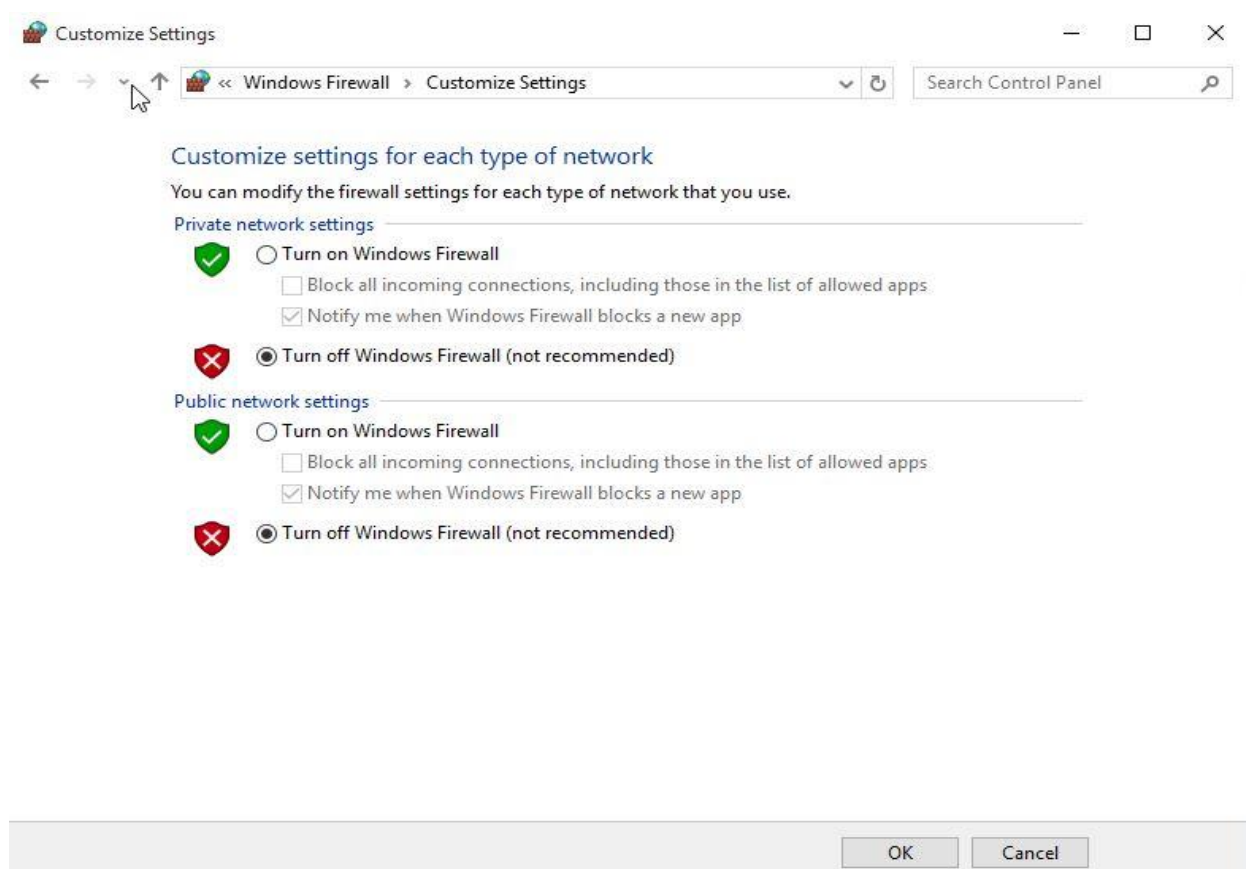




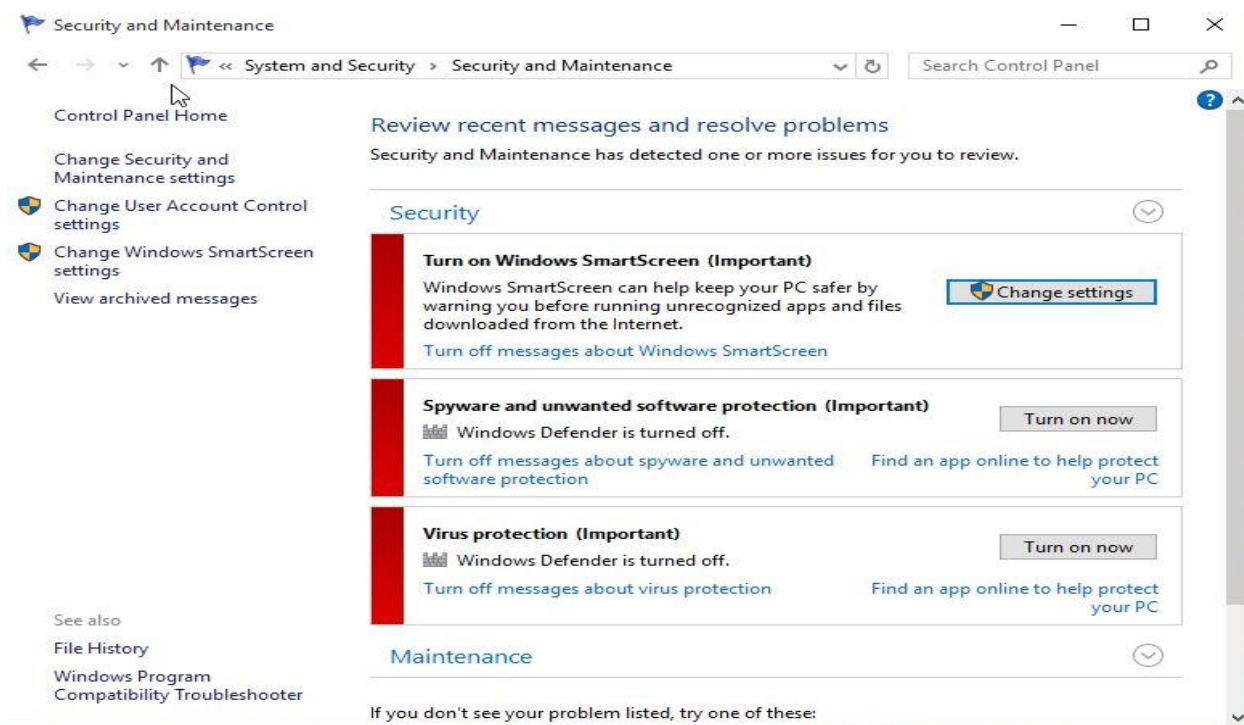
## Step 6: Now we have to disable the Windows Firewall settings



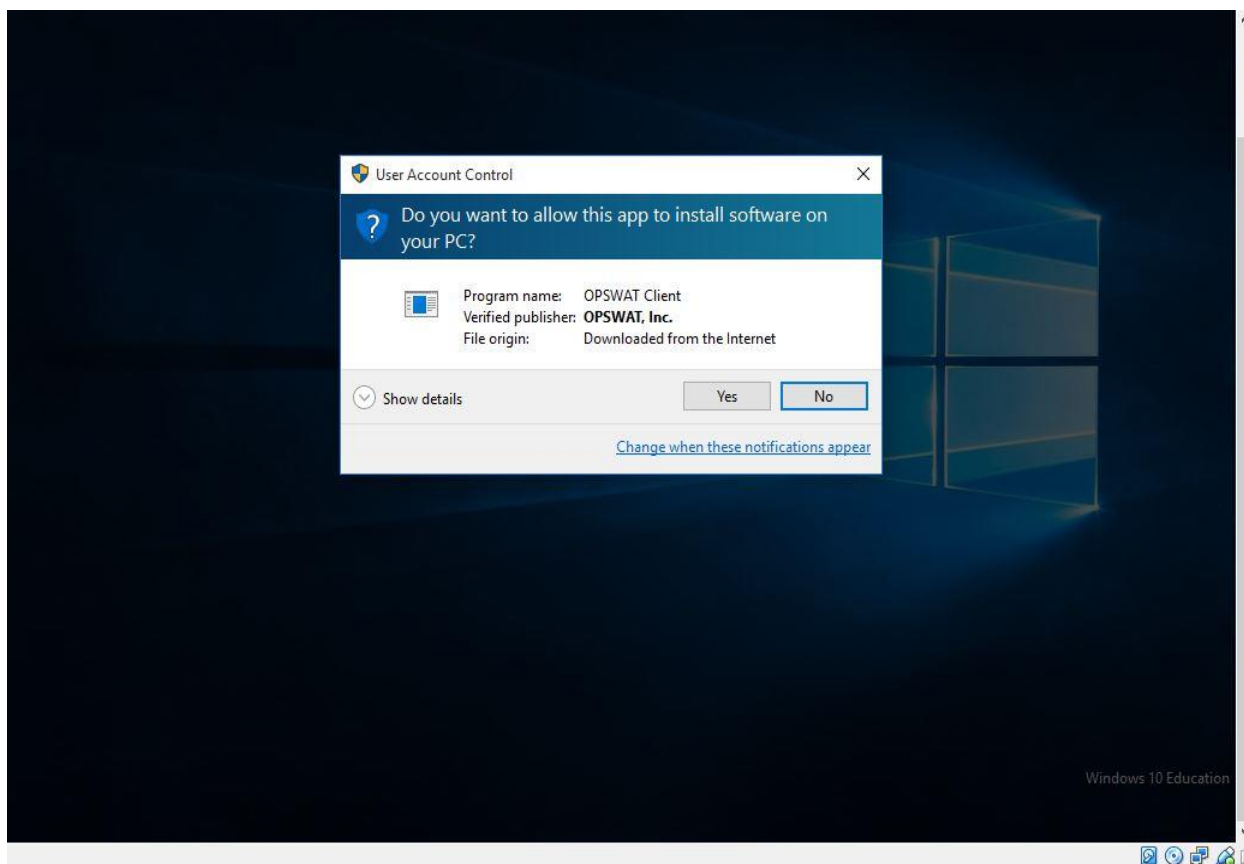
## Step 7: Go to Firewall & network protection and turn off each option under it



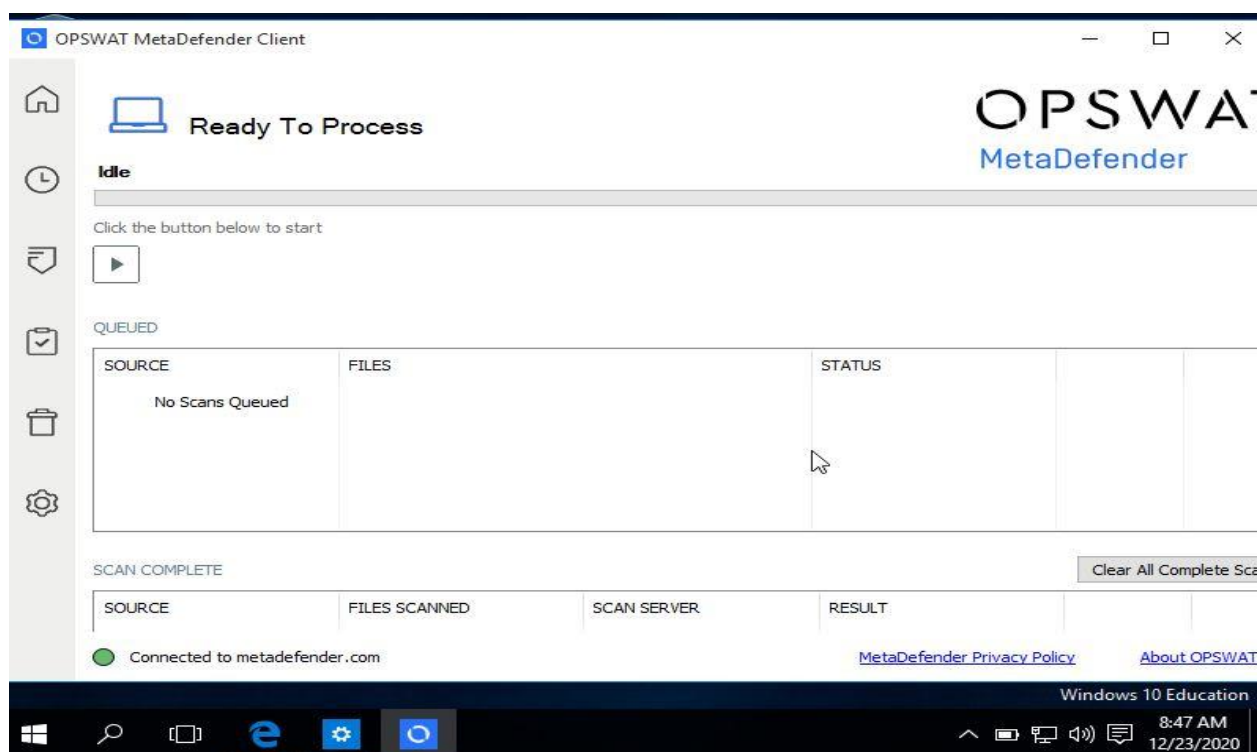
### Step 8: App and browser control settings will be turned off



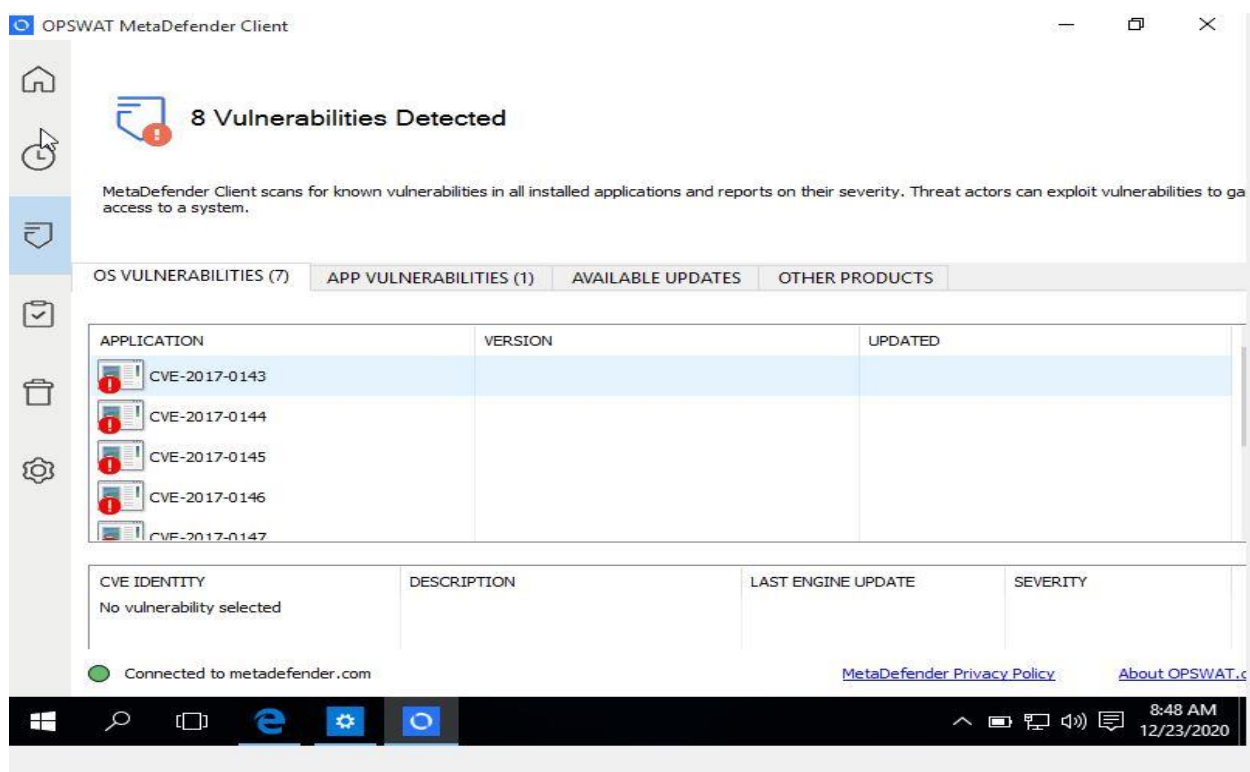
### Step 9: MetaDefender Malware opening (OPSWAT client)



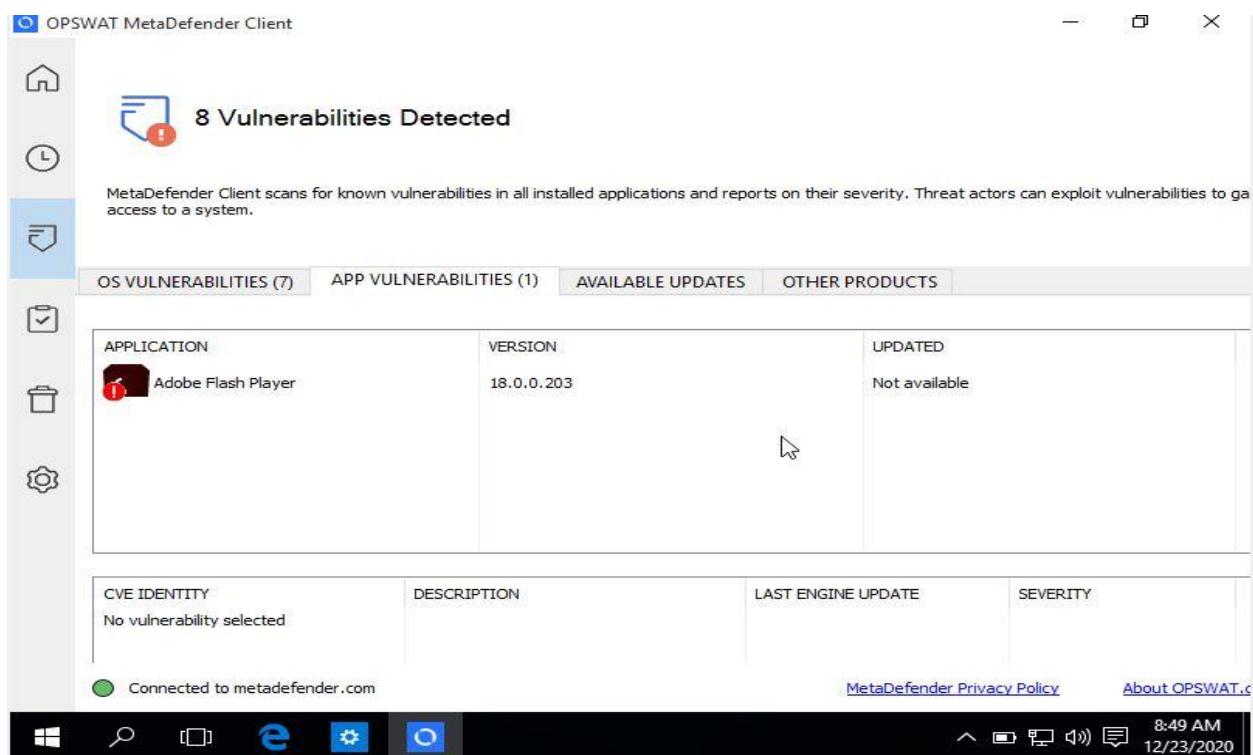
## Step 10: Metadefender client graphical user interface



**Step 11:** When you go to the Vulnerabilities tab (a down arrow) as shown below. Now you can see 7 OS vulnerabilities



## Now application vulnerabilities (1)




OPSWAT MetaDefender Client

**8 Vulnerabilities Detected**

MetaDefender Client scans for known vulnerabilities in all installed applications and reports on their severity. Threat actors can exploit vulnerabilities to gain access to a system.

OS VULNERABILITIES (7) | **APP VULNERABILITIES (1)** | AVAILABLE UPDATES | OTHER PRODUCTS

APPLICATION	VERSION	UPDATED
 Adobe Flash Player	18.0.0.203	Not available

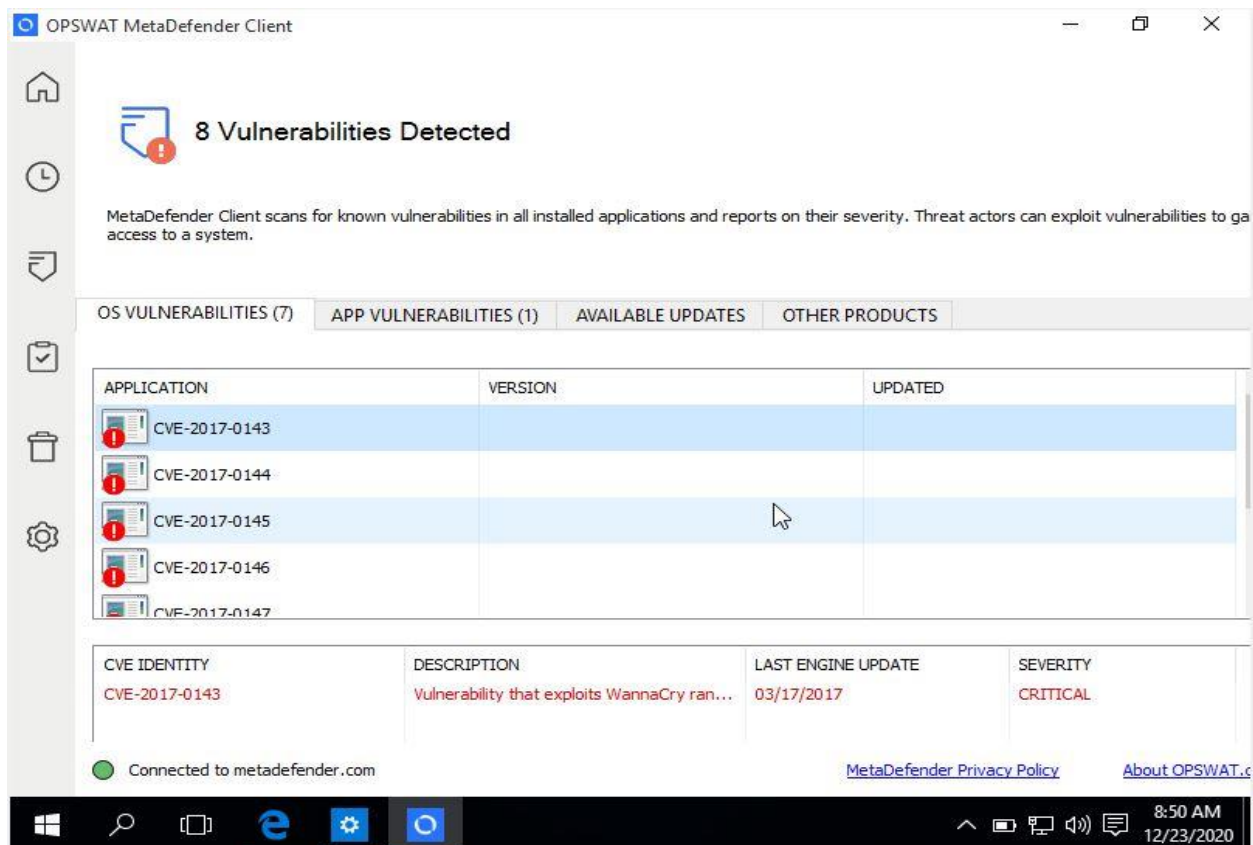
CVE IDENTITY	DESCRIPTION	LAST ENGINE UPDATE	SEVERITY
No vulnerability selected			

Connected to metadefender.com

[MetaDefender Privacy Policy](#) [About OPSWAT.c](#)

8:49 AM 12/23/2020

## Step 12: Analyzing the malware after detection








OPSWAT MetaDefender Client

**8 Vulnerabilities Detected**

MetaDefender Client scans for known vulnerabilities in all installed applications and reports on their severity. Threat actors can exploit vulnerabilities to gain access to a system.

OS VULNERABILITIES (7) | **APP VULNERABILITIES (1)** | AVAILABLE UPDATES | OTHER PRODUCTS

APPLICATION	VERSION	UPDATED
 CVE-2017-0143		
 CVE-2017-0144		
 CVE-2017-0145		
 CVE-2017-0146		
 CVE-2017-0147		

CVE IDENTITY	DESCRIPTION	LAST ENGINE UPDATE	SEVERITY
CVE-2017-0143	Vulnerability that exploits WannaCry ran...	03/17/2017	CRITICAL

Connected to metadefender.com

[MetaDefender Privacy Policy](#) [About OPSWAT.c](#)

8:50 AM 12/23/2020

OPSWAT MetaDefender Client

## 8 Vulnerabilities Detected

MetaDefender Client scans for known vulnerabilities in all installed applications and reports on their severity. Threat actors can exploit vulnerabilities to gain access to a system.

OS VULNERABILITIES (7)   APP VULNERABILITIES (1)   AVAILABLE UPDATES   OTHER PRODUCTS

APPLICATION	VERSION	UPDATED
Adobe Flash Player	18.0.0.203	Not available

CVE IDENTITY	DESCRIPTION	LAST ENGINE UPDATE	SEVERITY
CVE-2016-4151	Unspecified vulnerability in Adobe Flash ...	10/12/2018	CRITICAL
CVE-2018-12825	Adobe Flash Player 30.0.0.134 and earli...	10/30/2018	CRITICAL
CVE-2017-2069	Adobe Flash Player versions 25.0.0.149	01/04/2019	CRITICAL

Connected to metadefender.com

[MetaDefender Privacy Policy](#)   [About OPSWAT](#)

**Step 13:** Browse to the website <https://www.cvedetails.com/> on the machine to know the details of the vulnerability

CVE security vulnerability: X +

cvedetails.com/index.php

## CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

[Log In](#)   [Register](#)   [Vulnerability Feeds & Widgets](#)   [www.itsecdb.com](#)

Enter a CVE id, product, vendor, vulnerability type...

### Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	703	0.60
1-2	914	0.70
2-3	4880	4.00
3-4	4556	3.70
4-5	27455	22.20
5-6	23785	19.30
6-7	17054	13.80
7-8	27369	22.20
8-9	553	0.40
9-10	16185	13.10
<b>Total</b>	<b>123454</b>	

Weighted Average CVSS Score: 6.6

Vulnerability Distribution By CVSS Scores

CVSS Score Ranges

- 0-1
- 1-2
- 2-3
- 3-4
- 4-5
- 5-6
- 6-7
- 7-8
- 8-9
- 9-10

Looking for OVAL (Open Vulnerability and Assessment Language) definitions? <http://www.itsecdb.com> allows you to view exact



**Step 14:** Select one CVE and enter the number CVE-2017-0143 and click on Search button

The screenshot shows the CVE Details website interface. On the left, there is a sidebar with navigation links like Home, Browse, Reports, Search, and Top 50. The main content area shows the search results for CVE-2017-0143. A table titled 'Current CVSS Score Distribution For All Vulnerabilities' displays the distribution of all vulnerabilities by CVSS scores. A bar chart titled 'Vulnerability Distribution By CVSS Scores' shows the distribution of vulnerabilities by CVSS scores.

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	703	0.60
1-2	914	0.70
2-3	4880	4.00
3-4	4556	3.70
4-5	27455	22.20
5-6	23785	19.30
6-7	17054	13.80

**Step 15:** Details of the entered malware

The screenshot shows the CVE Details website interface for CVE-2017-0143. The page displays the CVE Details header, a search bar, and a detailed description of the vulnerability. It also includes a table of CVSS scores and vulnerability types.

**Vulnerability Details : CVE-2017-0143 (6 Metasploit modules)**

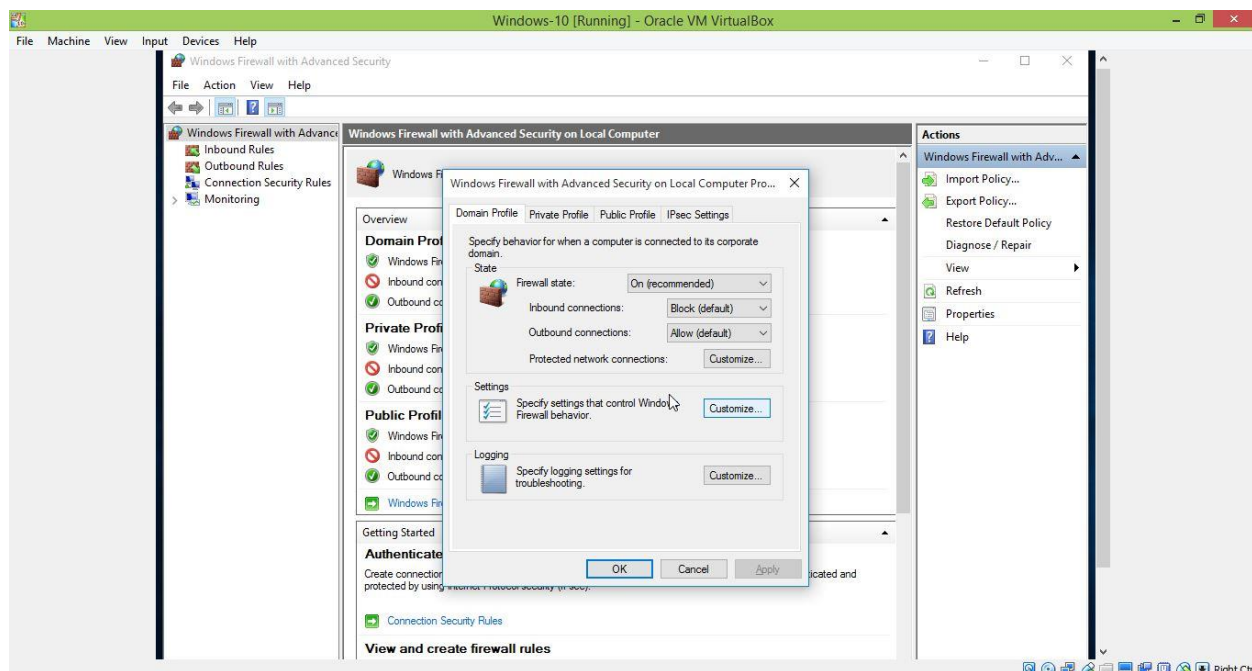
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Publish Date : 2017-03-16 Last Update Date : 2018-06-20

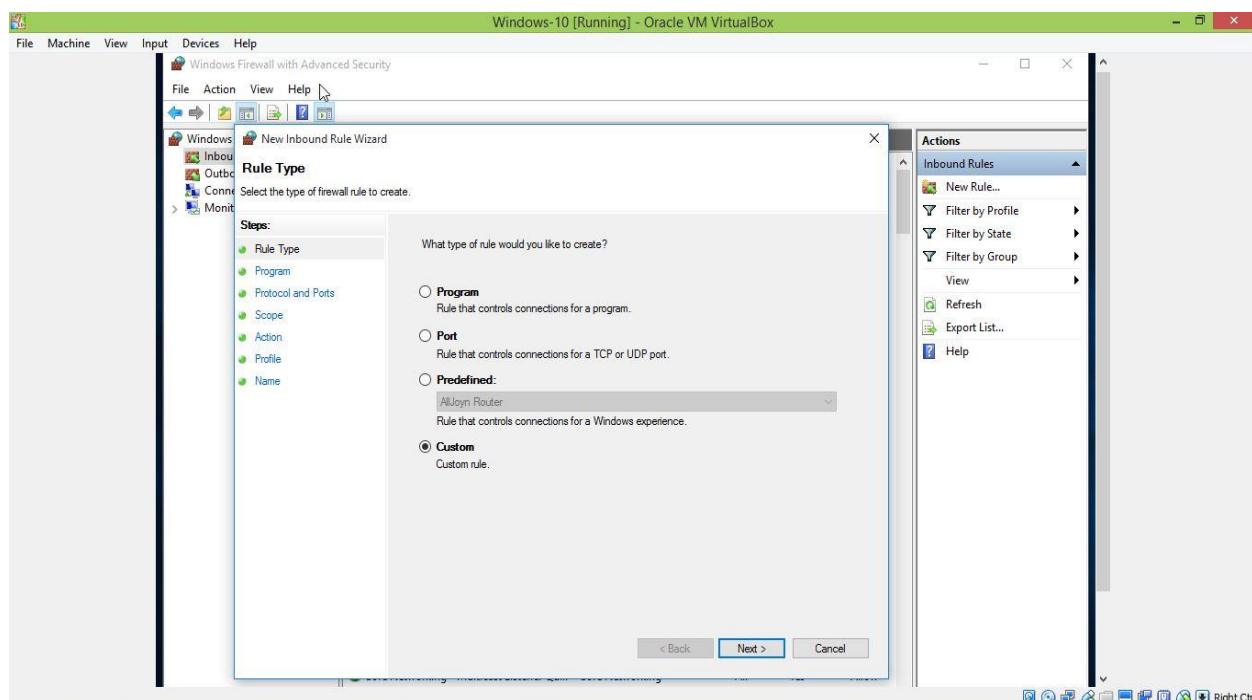
CVSS Score	Confidentiality Impact	Integrity Impact	Availability Impact	Access Complexity	Authentication	Gained Access	Vulnerability Type(s)	CWE ID
9.3	Complete (There is total information disclosure, resulting in all system files being revealed.)	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)	Not required (Authentication is not required to exploit the vulnerability.)	None	Execute Code	20

### Part Three: (Block the detected sample)

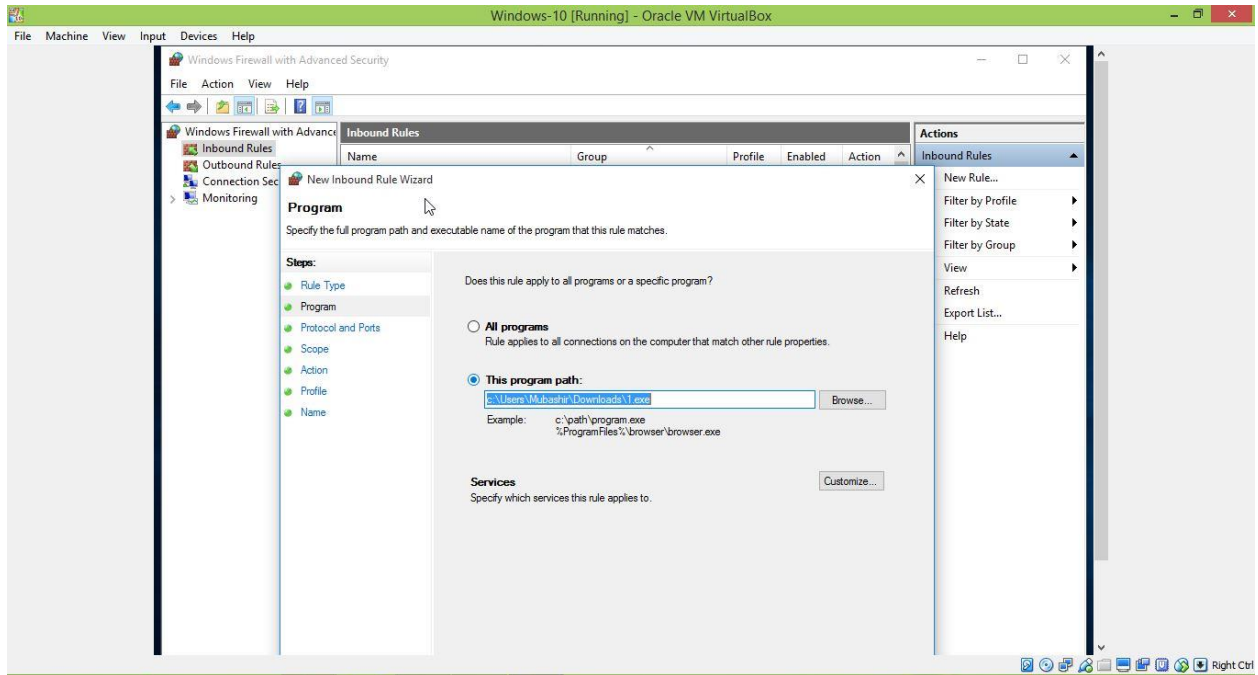
**Step 1:** After analyzing the malware now we want to block this malware from functioning using Windows Firewall settings



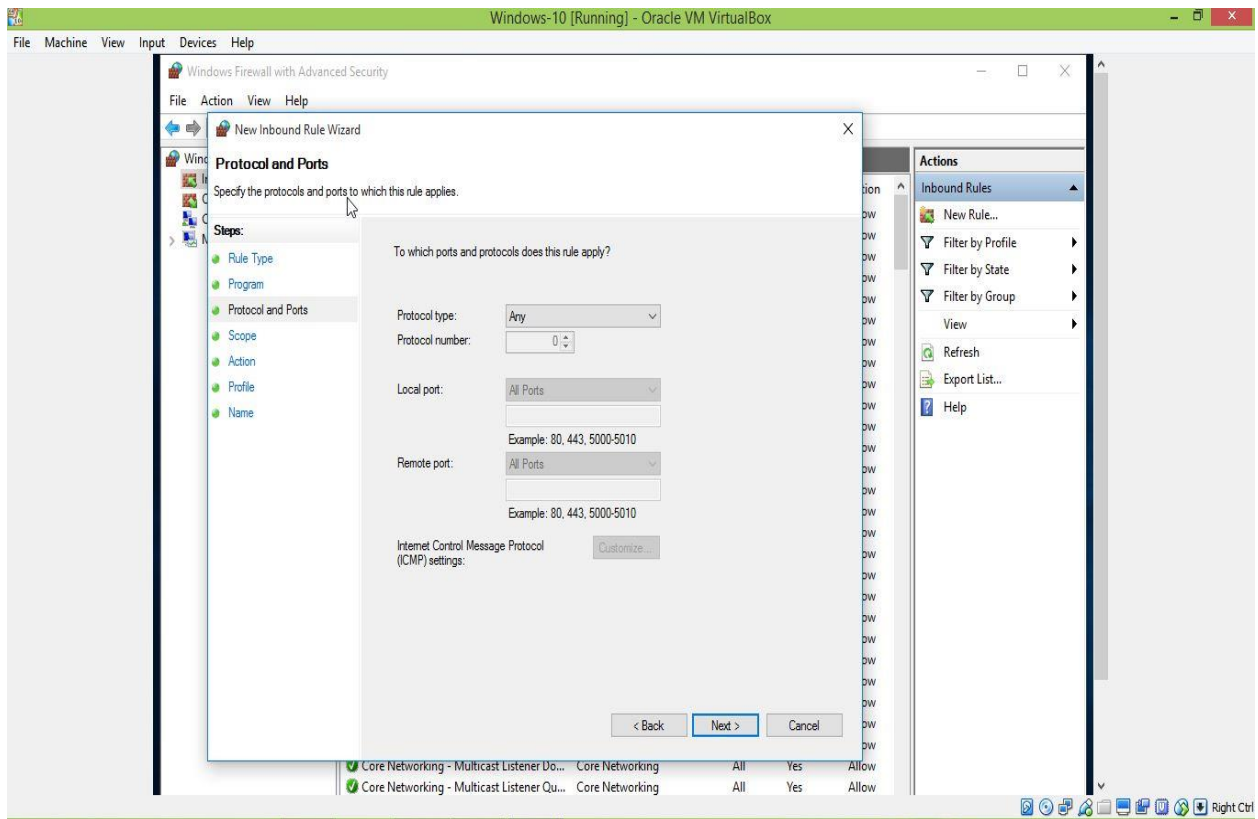
**Step 2:** In this step an inbound policy is created with the help of 'New Inbound Rule Wizard'. Under this wizard, select the rule type you want to create; as applicable. Now click on **Custom**.



**Step 3:** Now copy the sample malware path to the 'This program path' or browse to the location as shown below.

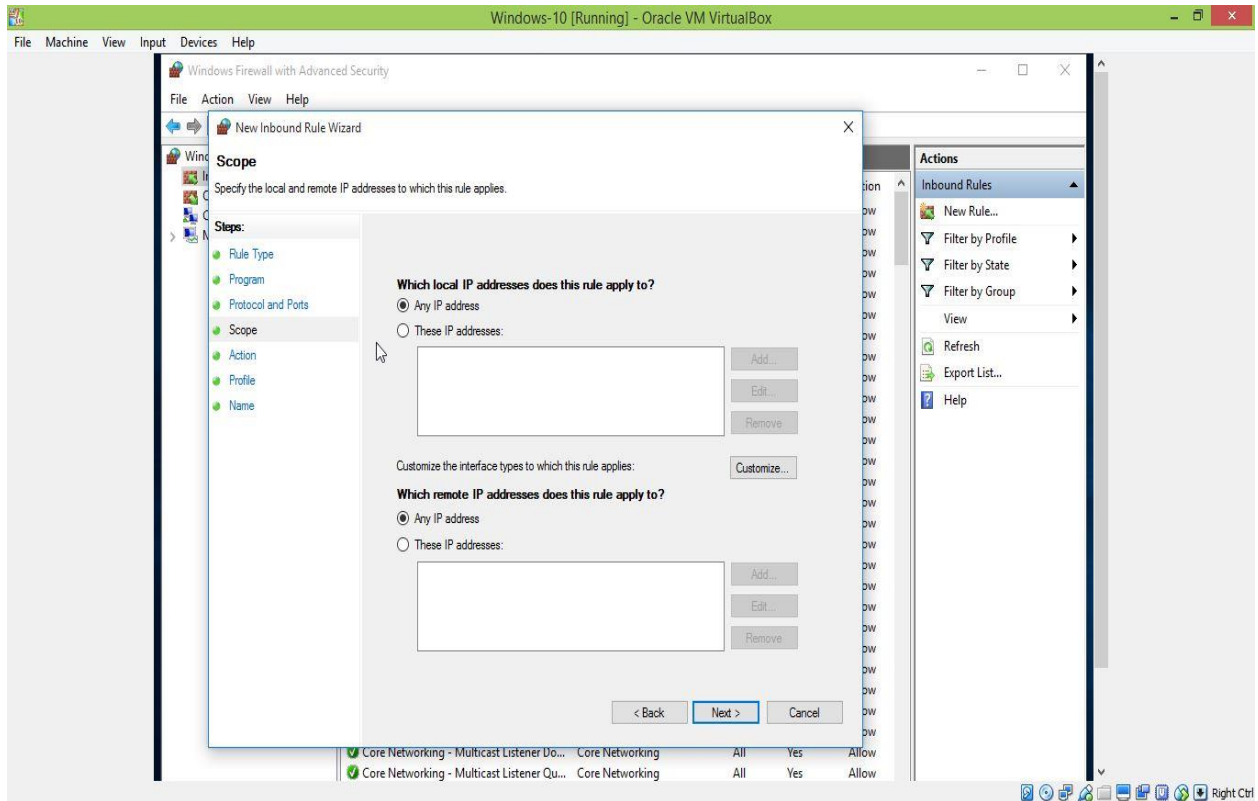


**Step 4:** If any protocol is enabled then select the Protocol and port tab. In our case no protocol

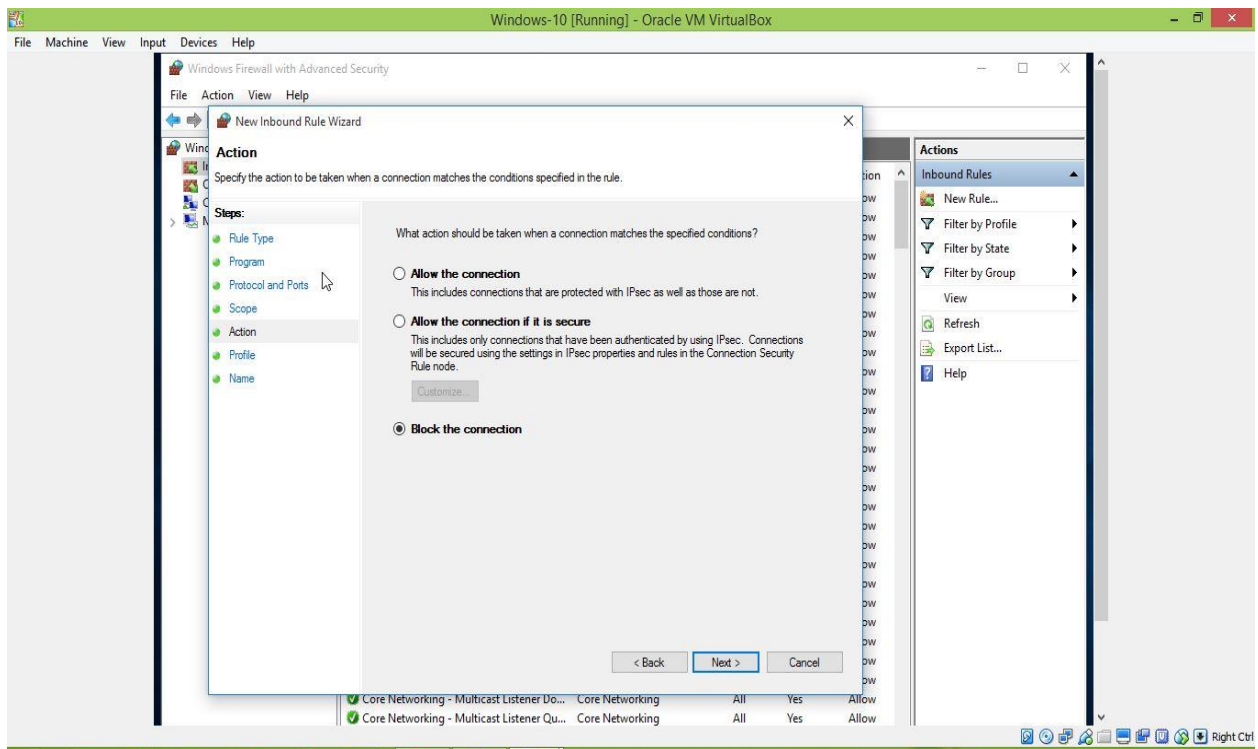




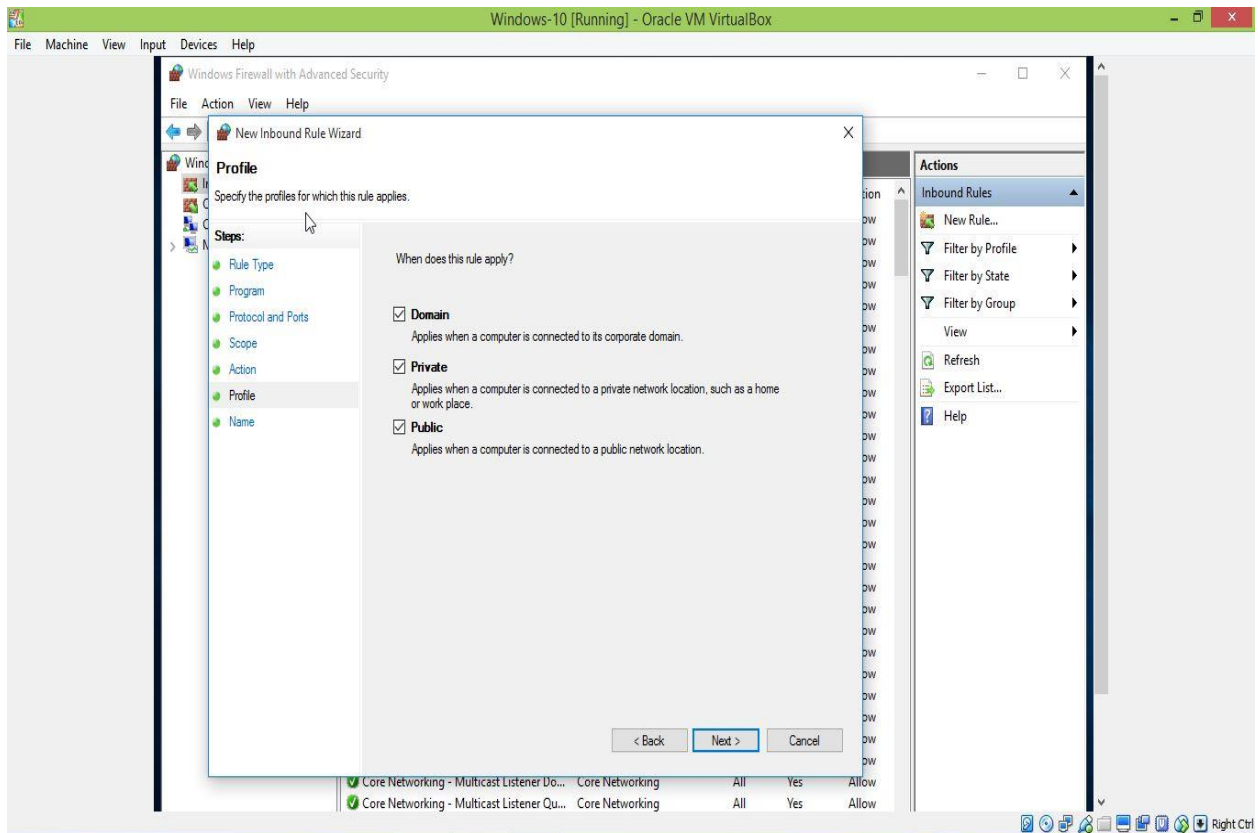
**Step 5:** Select the Scope of IP address; if any. We don't have any click **Next**.



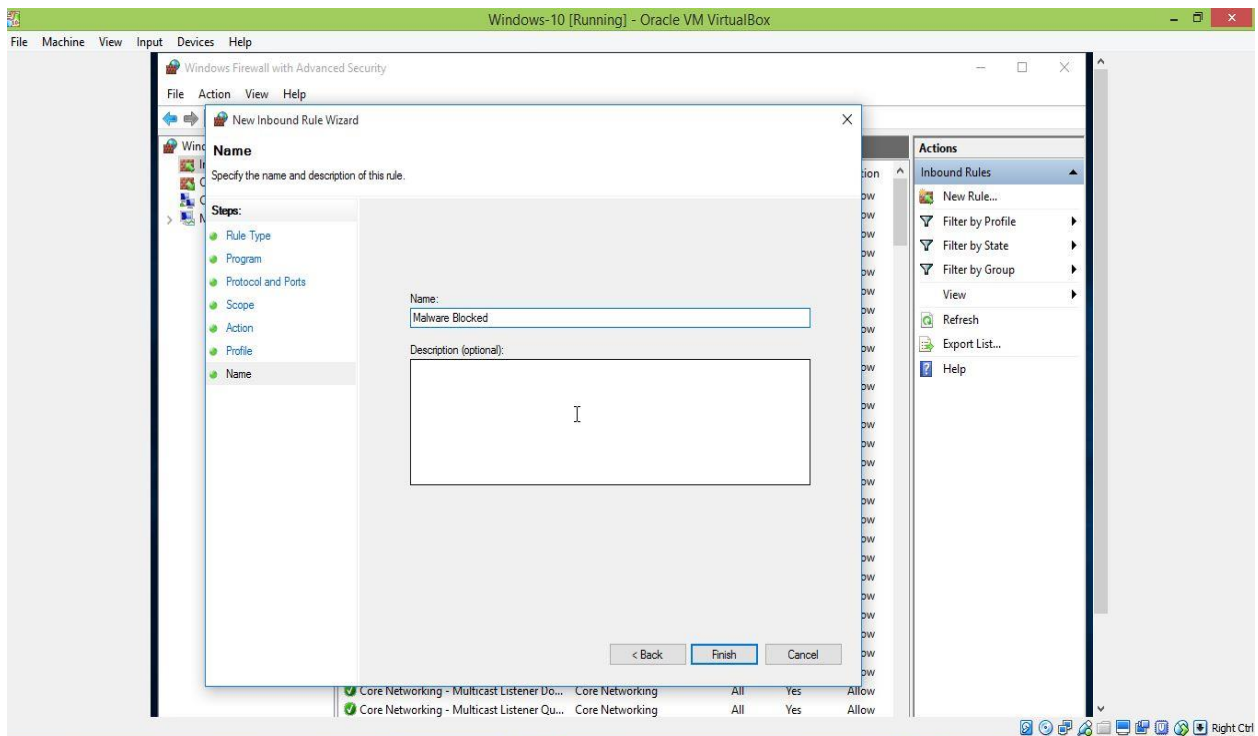
**Step 6:** Now select the radio button Block the connection. Click **Next**.



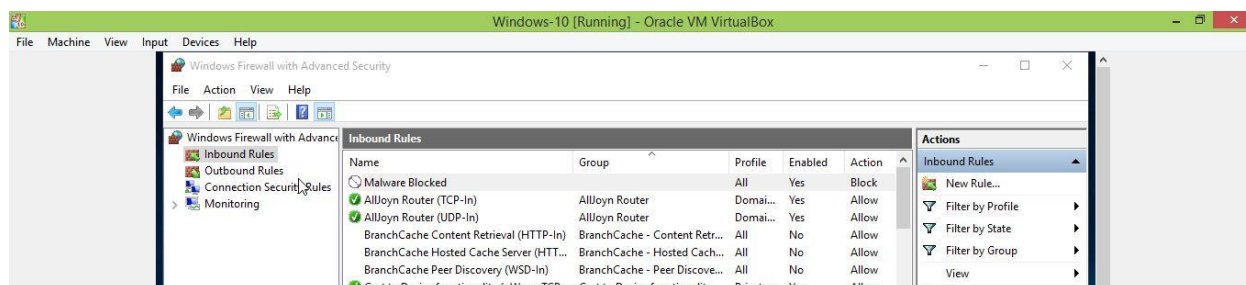
**Step 7:** After that check 'Check all the profile', on which this rule applies. Click **Next**.



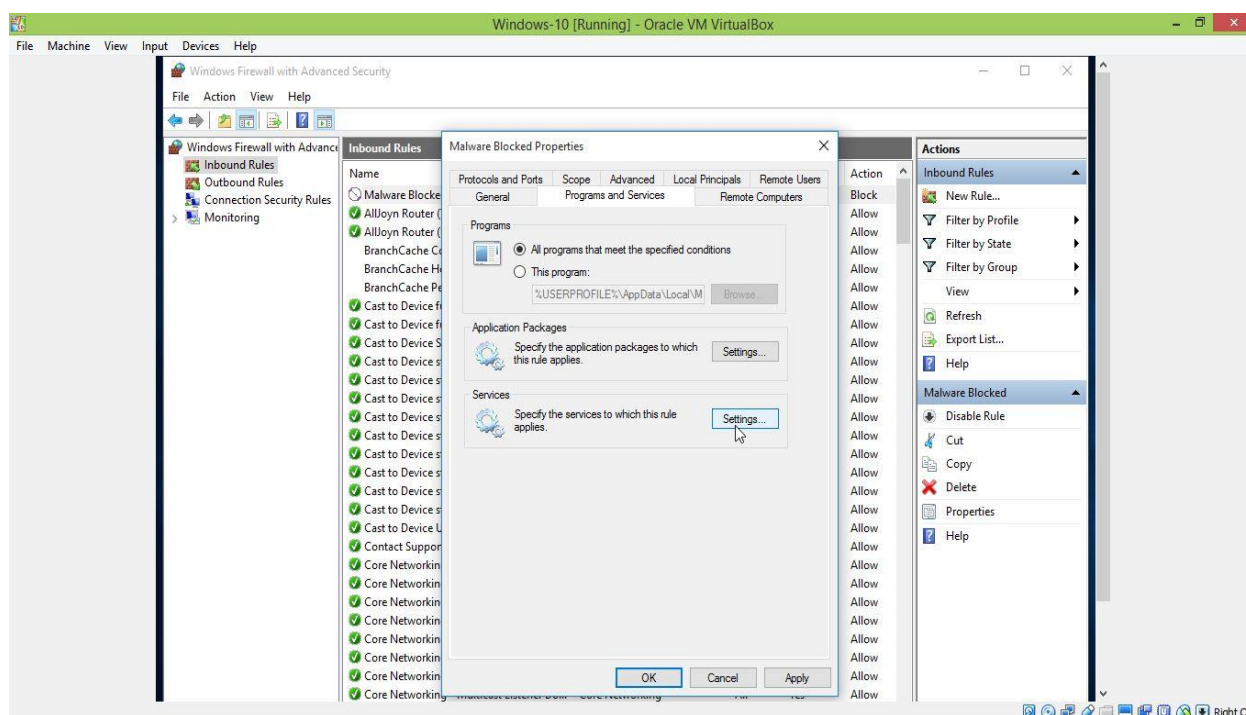
**Step 8:** Type any name for the Rule and click **Finish**



**Step 9:** Now the Blocked sample is seen



**Step 10:** Right click on the created rule and select its Properties. The details are here, now click OK.

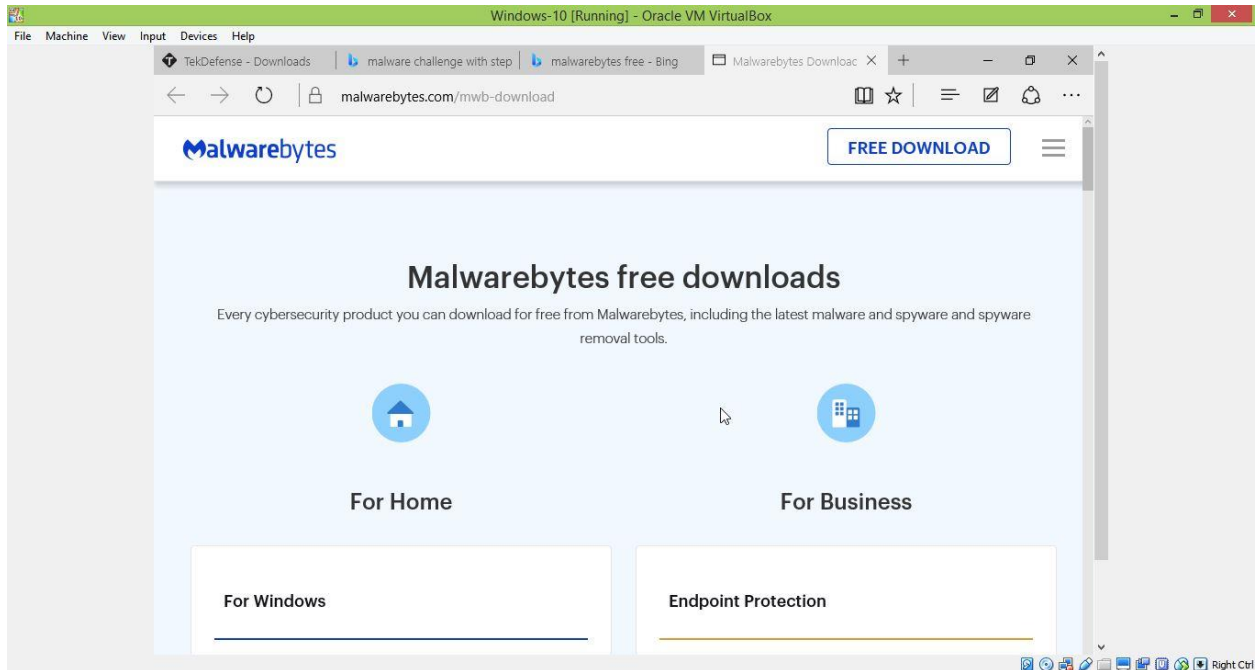


## Part Four: A challenge

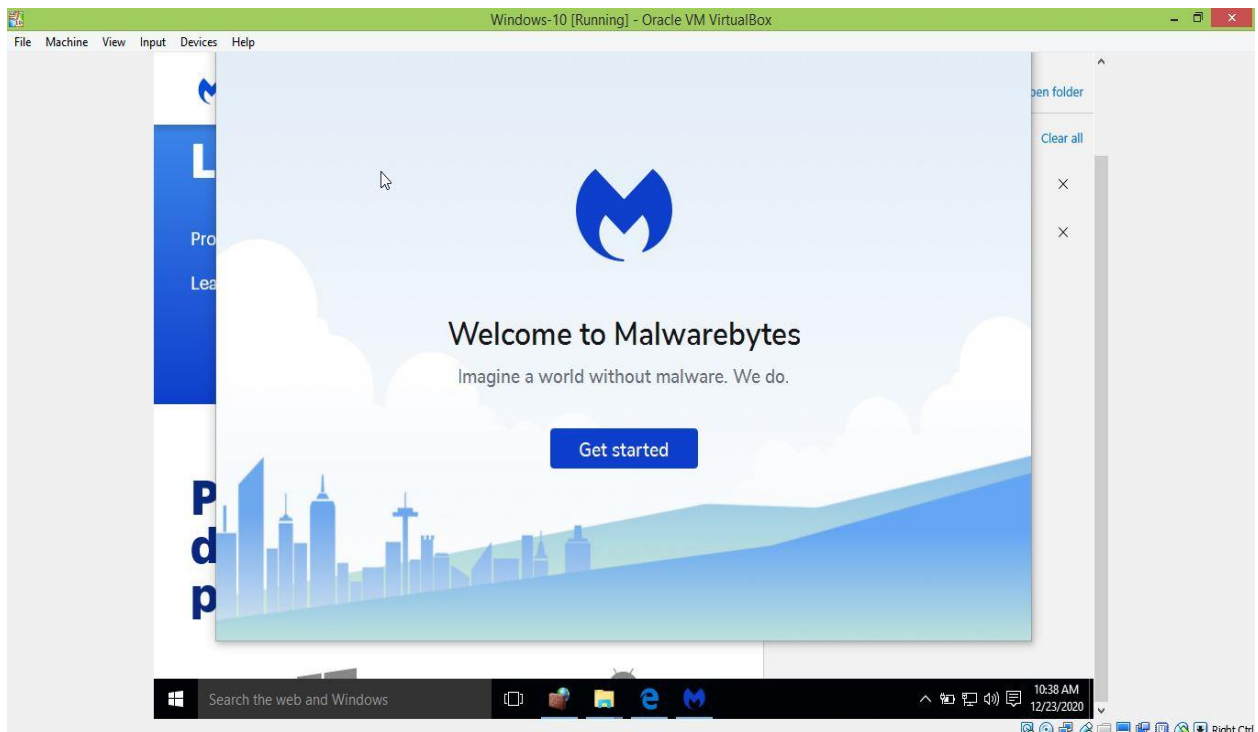
In this challenge I have downloaded the 'Malware bytes' software for scanning and performing vulnerability assessment. This software was paid. But the trial version is available. First, I will show the installation summary and second, I will show some samples of malwares and finally a complete defensive strategy will be followed. In the final part I will not show how to build a defensive strategy as it is demonstrated above and same for the challenge. For the time being, I will show the installation and samples of malwares. Hopefully, kindly, please consider this.

## Part ONE (Installation)

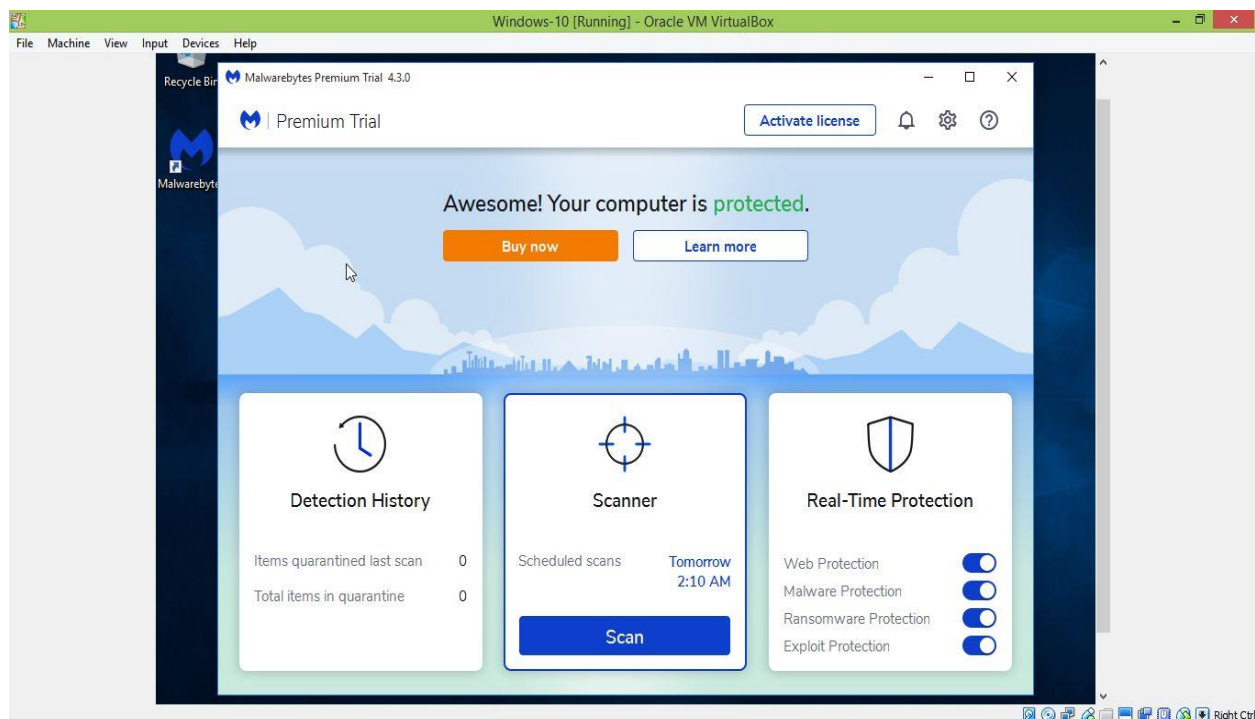
### Step 1: Download the 'Malwarebytes software from the internet'



### Step 2: Successful installation of the above mentioned software.

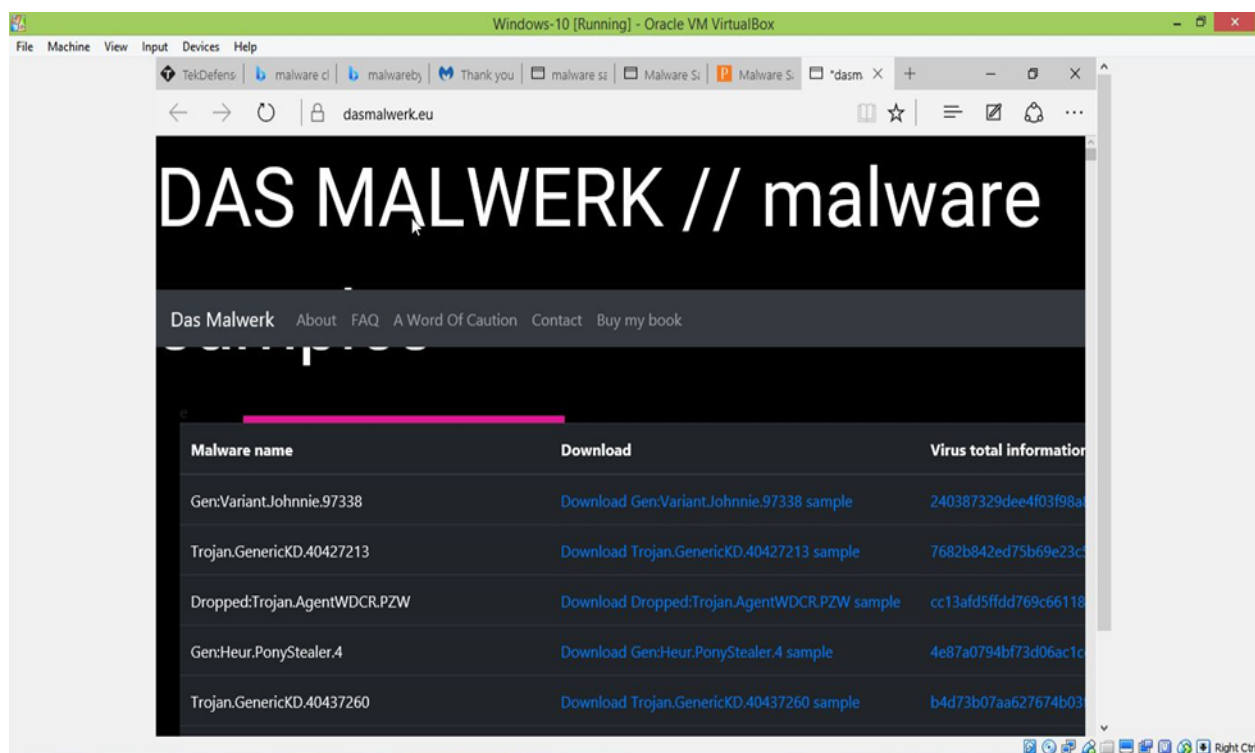


**Step 3:** After successful completion a dialogue will appear for scanning and finding vulnerability.



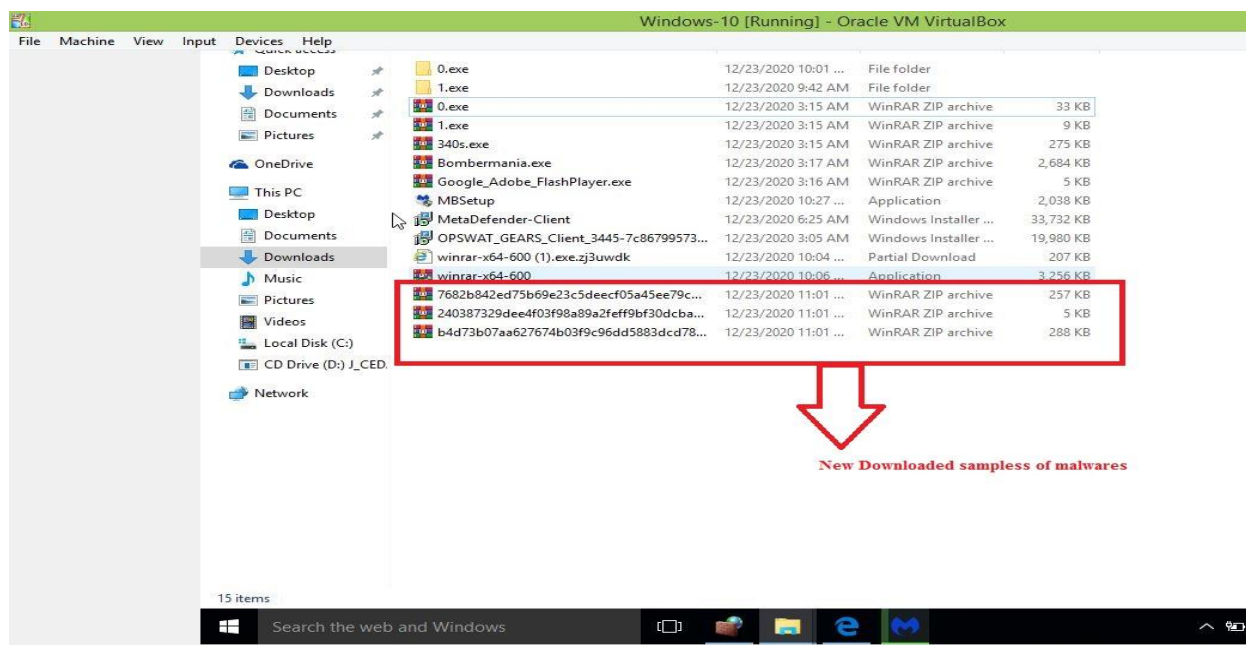
## Part TWO (Downloading samples)

**Step 1:** Browse the website <https://www.dasmalwerk.eu> to download the samples





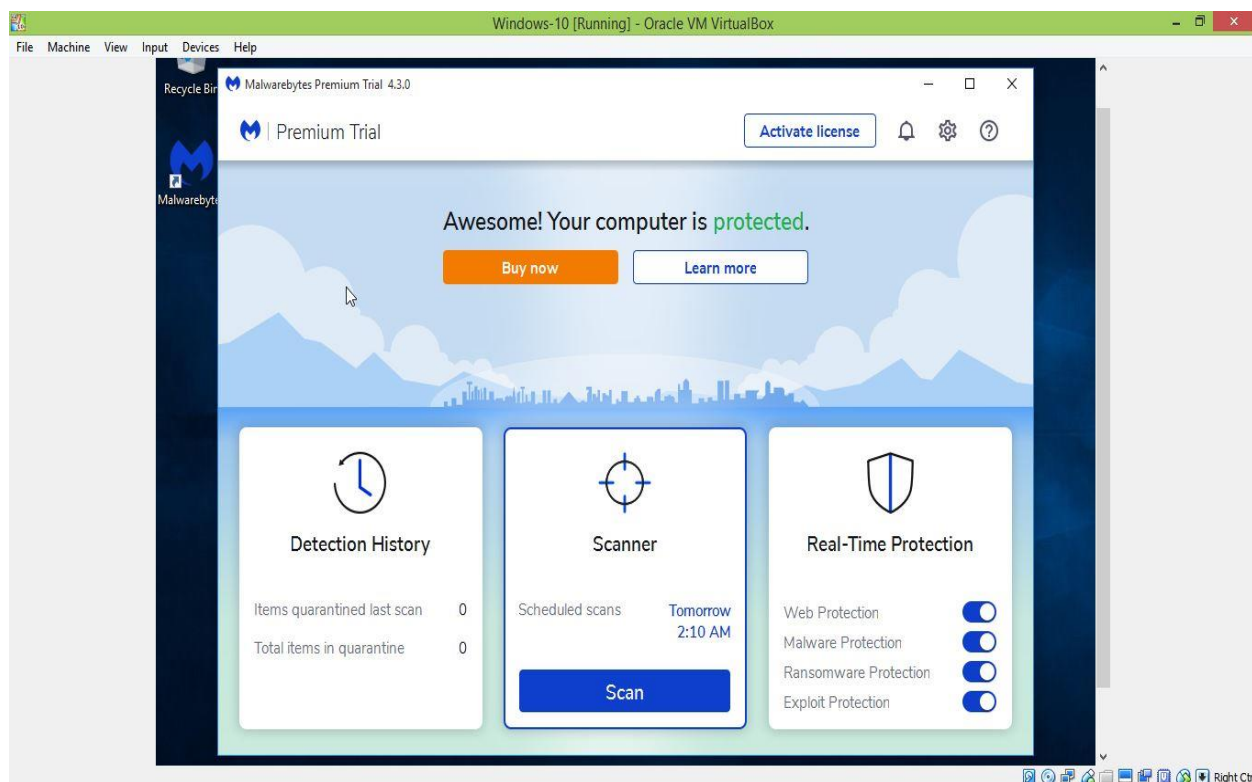
## Step 2: Showing the downloaded samples of malwares



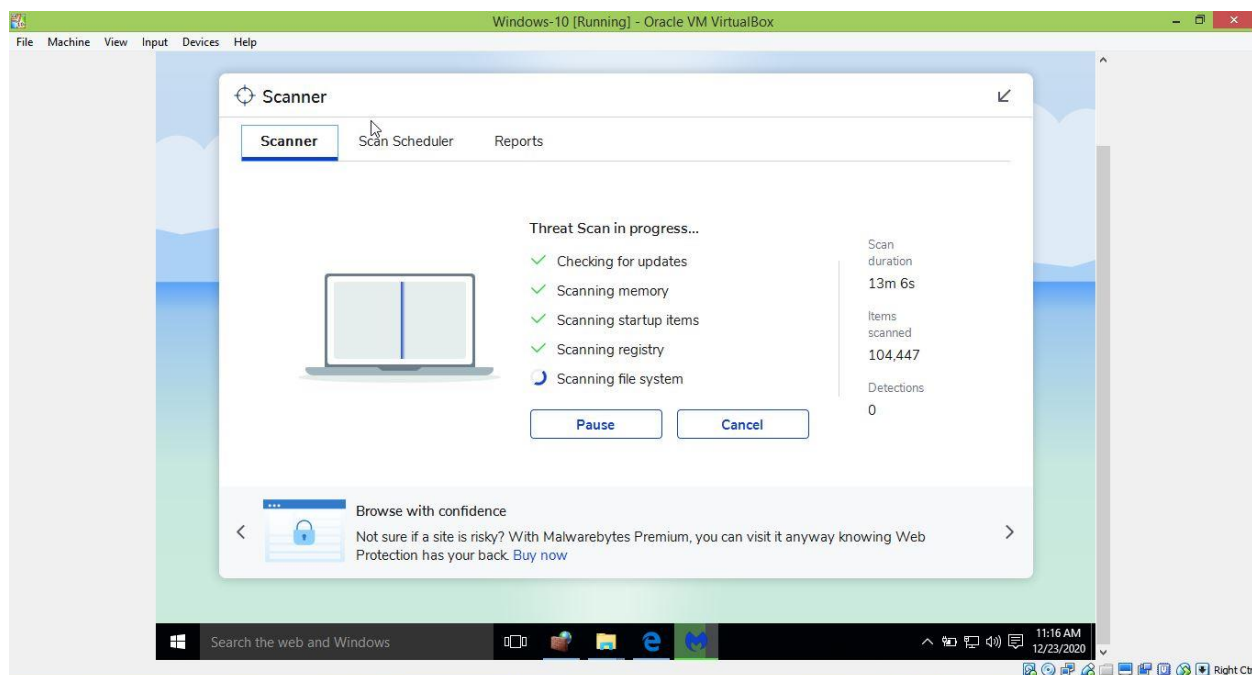
**Step 3:** In this step, we have to find the details of the malware. Here in this challenge encrypted names were found so it was difficult to find the details without their name.

## Part THREE (Scanning)

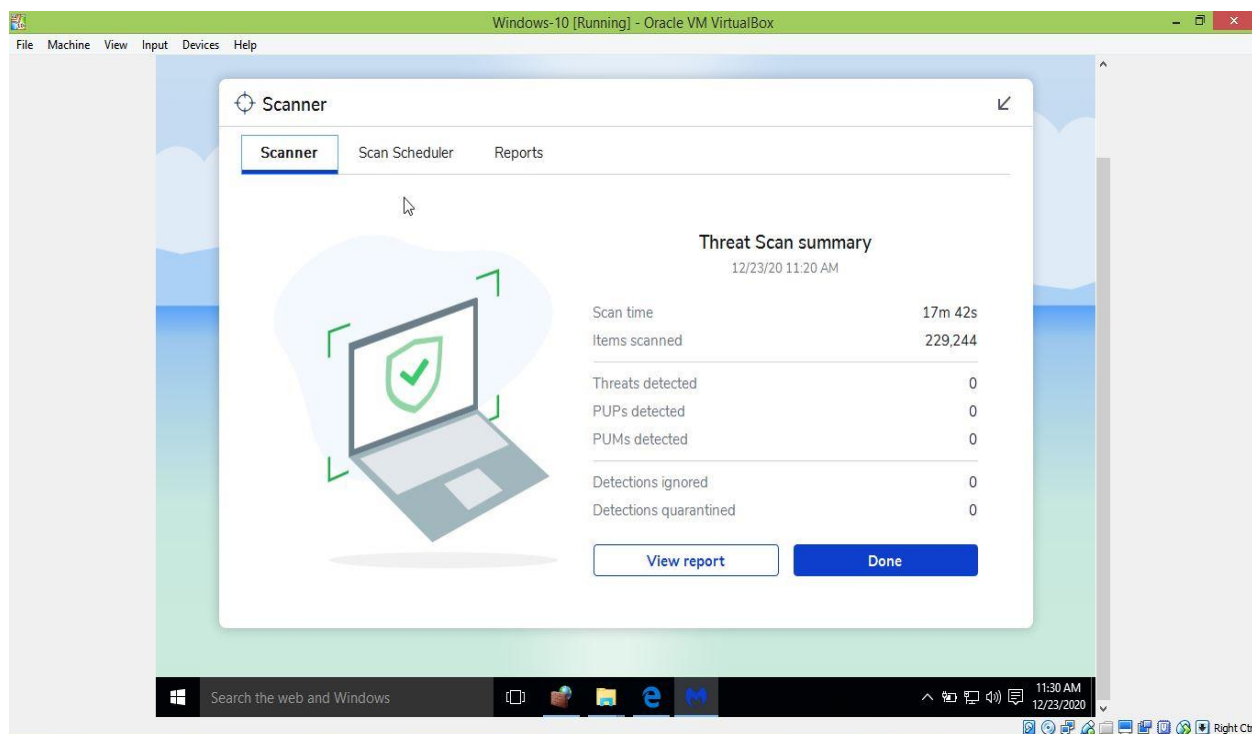
**Step 1:** Selecting the scan menu from the GUI of Malware bytes software



## Step 2: Starting the scan



## Step 3: Finished scanning



**Note:** This software didn't find the vulnerabilities because it works perfect when we purchase it. From my experience, that's why it didn't fetch the require results.

#### **Part 4: Building the defensive strategy**

In our case, a defensive strategy can be built, but this software finds the vulnerabilities and block them if we purchase it. The steps followed will be the same as described above in Part 3.

**Question 2: a) Please write your own reflection on the whole lab assignment.**

**Answer:** The whole assignment was a great experience. By learning how to build a defensive strategy was the most interesting part. Being an information security student, these Labs provide a great exposure of industry practical knowledge. Learning is successful if it is accompanied by practical experience. From the beginning of this assignment to the end, it was an excellent learning work and experience. Hopefully, it will help me in keeping my grip strong on information security concepts and experience.

**Question 3: What is your reflection on the entire week of the course?**

**Answer:** The coursework of this week of the subject 'Applied computer security' was good. The theory along with practical lab was a good step in the right direction. Learning new concepts is always good. Looking forward for such a good experience in future.