WEEK 3 – TASK 3.3D

Distinction Task.
Release Date: 29 March, Due Date: 15 April, End Date: 19 April.

Learning Outcomes

In this task, you will learn about penetration testing. You will learn about Ethical Hacking, Metasploit framework, Metasploitable, and will practice basic penetration testing.

Instructions

Resources

An **answer sheet template** is available on OnTrack as a `**Resources**’. Please download the answer sheet and fill it with your answers. To upload on OnTrack, you need to convert the answer sheet template document to **PDF**. MS Word includes built-in PDF conversation capability.

We are fighting the good fight. We are on the good side of the cyber world and we are in this together. We learn together and from each other.

Help is always available in SIT182. Please go to **Discussions** and ask your questions about this task in **Task 3.3D**. All students are encouraged to participate and help peers with their questions. Helping others is a great way to learn and think about aspects you may have overlooked. You can also seek help from tutors during online and face-to-face pracs. However, please note that pracs are primarily aimed for Pass-level tasks and tutors will only aim to provide you with suggestions about the more advanced tasks.

Note: Distinction tasks are more challenging and are less guided. The only source of support for Distinction-level tasks is Discussions on the unit site. Students who achieve Distinction in this unit are top performers in Bachelor of Cyber. You will need to show dedication, professionalism, and ambition to complete Distinction tasks. If you start working on this task the night before deadline, it is very unlikely for you to be able to complete it.

References: In cyber security, one of the most common referencing styles is **IEEE** – however, you are allowed to use any referencing style in this unit. Please refer to unit site > Content > Referencing - Hints & Tips for more information.

The term "ethical hacker" might seem like an oxymoron—sort of like an ethical pick pocket or ethical embezzler. Ethical hackers are employed or contracted by a company to do what illegal hackers do: break in. Why? Companies need to know what, if any, parts of their security infrastructure are vulnerable to attack. For example, to protect a company's network, many security professionals recognize that knowing what tools the bad guys use and how they think enables them to better protect (harden) a network's security.

In a penetration test, an ethical hacker attempts to break into a company's network or applications to find weak links. In a vulnerability assessment, the tester attempts to enumerate all the vulnerabilities found in an application or on a system. In a security test, testers do more than attempt to break in; they also analyze a company's security policy and procedures and report any vulnerabilities to management. Security testing, in other words, takes penetration testing to a higher level. As Peter Herzog states in the Open-Source Security Testing Methodology Manual, "[Security testing] relies on a combination of creativeness, expansion [of] knowledge bases of best practices, legal issues, and client industry regulations as well as known threats and the breadth of the target organization's security presence (or point of risk)."

i

An ethical hacker is a person who performs most of the same activities a hacker does but with the owner or company's permission. This distinction is important and can mean the difference between being legally charged with a crime or not being charged.

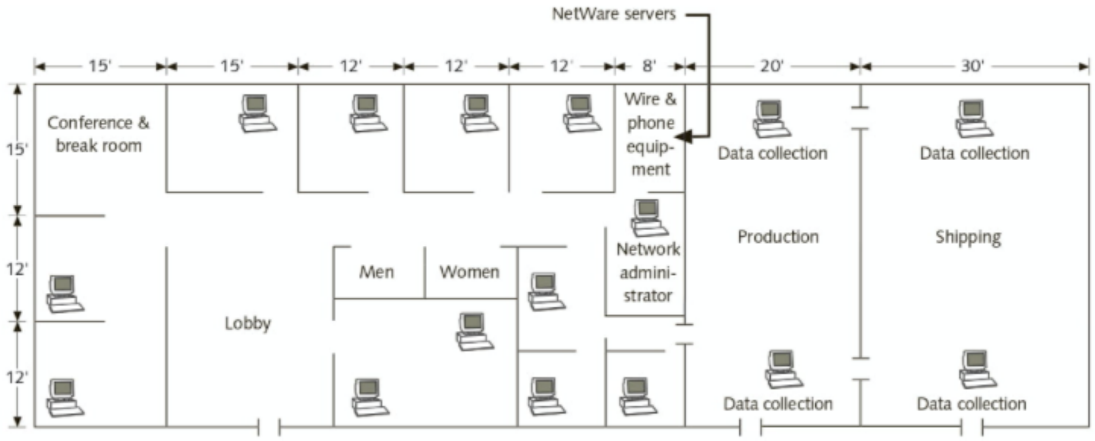
These issues are just some of the one's security testers must examine. In doing so, they alert companies to areas that need to be monitored or secured. As a security tester, you can't make a network impenetrable. The only way to do that with certainty is to unplug the network cable. When you discover vulnerabilities ("holes") in a network, you can correct them. This process might entail tasks such as updating an operating system (OS) or installing a vendor's latest security patch.

If your job is a penetration tester, you simply report your findings to the company. Then it's up to the company to make the final decision on how to use the information you have supplied. However, as a security tester, you might also be required to offer solutions for securing or protecting the network.

Ethical hackers who perform penetration tests use one of these models:

- White box model
- Black box model
- Gray box model

In the white box model, the tester is told what network topology and technology the company is using and is given permission to interview IT personnel and company employees. For example, the company might print a network diagram showing all the company's routers, switches, firewalls, and intrusion detection systems (IDSs) or give the tester a floorplan detailing the location of computer systems and the OSs running on these systems (see the following figure as an example).



This background information makes the penetration tester's job a little easier than it is with using the black box model. In the black box model, management doesn't divulge to staff that penetration testing is being conducted, nor does it give the tester any diagrams or describe what technologies the company is using. This model puts the burden on the tester to find this information. This model also helps management see whether the company's security personnel can detect an attack.

The gray box model is a hybrid of the white and black box models. In this model, the company gives the tester only partial information. For example, the tester might get information about which OSs are used but not get any network diagrams.

Enough talking!

In this task, you will learn how to use Metasploit to gain access to a remote machine. The goal is to experience the basics of practical penetration testing. The Metasploit Framework (MSF) contains a collection of exploits. It's an infrastructure that you can build upon and utilize for your custom needs. This helps you to concentrate on setting up your exploitation environments, and not have to reinvent the wheel. MSF is one of the most popular tools for security professionals conducting practical hacking studies. It contains an extensive exploitation tools and working environments. Additionally, it is free available to public.

You will use two Linux virtual machines: One is a Kali Linux with Metasploit framework installed; and the other one is intentionally vulnerable Linux known as Metasploitable. We will use the Metasploit framework on Kali Linux to remotely gain access on the vulnerable Linux machine.

- You already have Kali VM from Task 1.4P.
- Metasploitable 2 is available from: https://docs.rapid7.com/metasploit/metasploitable-2/

You will find documentation for Metasploitable through the same link. Before getting started browse through the page, which includes information on how to login to Metasploitable 2, obtaining IP, and a handy guide by HD Moore.

Ensure both VMs are connected to "Bridged Adapter" in the settings of VirtualBox. Next, run both of the VMs (i.e., Kali and Metasploitable 2) and then login to both VMs (remember the Metasploitable password is available to you through the link you download it and the documentation). [hint: you may want to try NAT or Internal Network if the two VMs couldn't reach each other or exploit was not working]

In Kali VM

Metasploit Framework uses PostgreSQL as its database, so you need to launch it by running the following command in the terminal. Run the Terminal in your Kali VM. Then, run

```
sudo service postgresql start
```

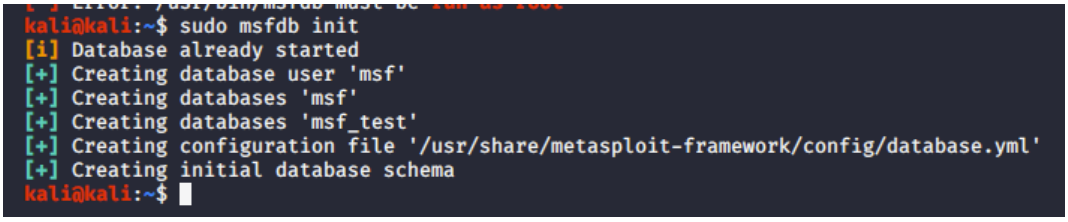
You can verify that PostgreSQL is running by executing the following command:

```
service postgresql status
```

With PostgreSQL up and running, you need to create and initialize the msf database by executing the following command:

```
sudo msfdb init
```

You should something like following:

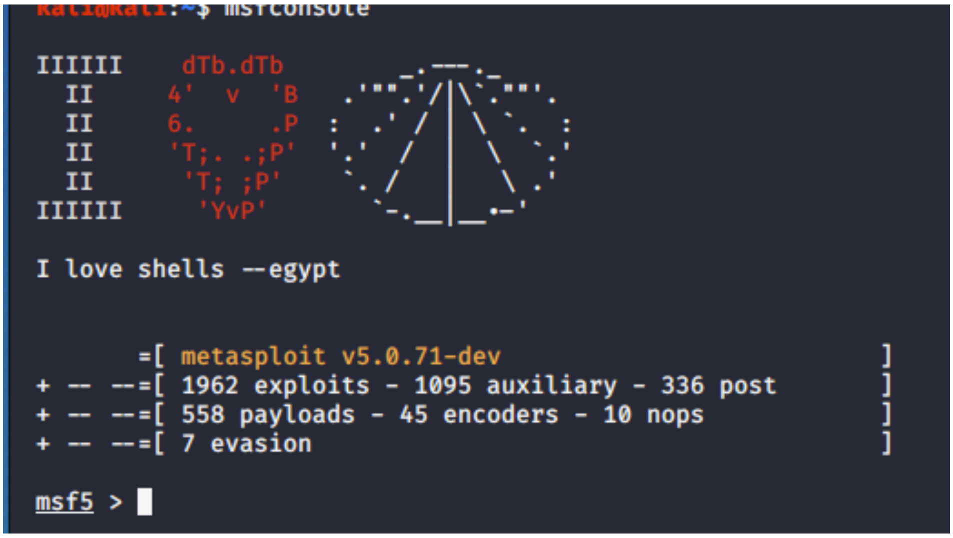


```
[-] Error: /usr/bin/msfdb must be run as root
kali@kali:~$ sudo msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
kali@kali:~$ 
```

Lunch the Metasploit console by running the following command in the terminal:

msfconsole

You should get something like below:



```
kali@kali:~$ msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v5.0.71-dev                          ]
+ -- --=[ 1962 exploits - 1095 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > 
```

Verify if the database is connected using the following command in msfconsole

db_status

Type help in msf console, you get the core and database commands.

You can find more information on how to use msfconsole from https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/

In Metasploitable VM

This VM is your victim (i.e., you are targeting this VM from Kali).

First, we need to find the host IP address of the target to launch a remote exploitation. You can use the command "ip a" or "ifconfig" (whichever works). Once you identify the IP address of the Metasploitable VM, make a note of it.

You now have your attacker (Kali VM) and know the IP of your vulnerable target. The rest is just using Metasploit to exploit a vulnerability and attack the target.

Question 1: You will need to find a vulnerability in Metasploitable 2 that allows backdoor access (i.e., full shell access) and exploit them through Metasploit running on Kali VM.

- You will need to use Metasploit documentation and your own research online to identify the vulnerability - Any vulnerability that grants backdoor access will meet the requirements of this question.

Hint: the logic of commands on Metasploit is going to be as follows: "Use [exploit/..] -> set RHOST [ip] -> set payload [..] -> exploit" then if you are successful, you will have shell access and can run `whoami' and `uname -a'.

You will need to show that you have managed to exploit the vulnerability and secured access to the target. Create a file on the victim machine by executing the following command: `touch [student ID]', where [Student ID] is your Deakin Student Number.

If you don't know what do, patiently see what you find online (there is plenty of information about this task online). You can always share interesting resources you find on Discussion (topic: Task 3.3D). *Remember, you will need to spend extra time and work more independently for Distinction asks – others before you have managed, and you will do too (as long as you are motivated and committed).*

(see next page for what you need to submit)

To answer this question, you will need to record your screen showing all steps up to Question 1 (i.e., running both VMs, login to both, getting Metasploit up and running, and the commands used to exploit the victim in Metasploit). You will then need to upload the video on Microsoft OneDrive, Google Drive, DropBox, or YouTube and share a link to your video. To screen record you can use any software of your choosing depending on your host OS. Here is one free suggestion: https://screencast-o-matic.com/screen-recorder

Important: if you use YouTube, you will need to ensure the privacy of video is set as **unlisted**. Further, the title of the video must be set as **Task 3.3D (2021).** Otherwise, the video will be available to anyone who searches the video, and it will be a case of academic integrity violation. Here is a guide on how to set privacy as unlisted: https://wiki.umbc.edu/pages/viewpage.action?pageId=31198917

Important: It is mandate by the School of IT that the unit chair has to conduct random 1-1 meeting with those submitting Distinction tasks to prevent academic integrity violation. This is to that the rights of those who spend time and effort is preserved. If you violate academic integrity and do not attend the 1-1 meeting, your task will be failed on OnTrack and further action may be taken by School of IT.

⚠ **Question 2: Reflection Point -** How difficult did you find the task? What resources you used to get the task done?