E.H UNIT - I

CO1:- Explain the concepts related to hacking, ports and protocols, pentesting and virtualization.

Syllabus:- Introduction to Hacking:- Hacking, Types and Phases of hacking, Introduction to ports & protocols :- ports, protocols, primary Networks types, Virtualization & Introduction to kali Linux :- Virtualization, Virtualization software, supported platforms, Introduction to penetration testing:- Penetration test, categories and types of penetration tests, structure of penetration test Report.

→ Hacking:- Ethical hacking is to crack passwords or to steal data? No, it is much more than that. Ethical hacking is to scan vulnerabilities and to find potential threats on a computer or network.

An ethical hacker finds the weak points or loopholes in a computer, web application or network and reports them to the organization. so, let's explore more about ethical hacking step by step.

→ Types of hackers:-

* White Hat Hackers (cyber - security Hacker)
* Black Hat Hackers (cracker)
* Gray Hat Hackers (Both)
* Blue Hat Hackers
* Green Hat Hackers
* Red Hat Hackers

* White Hat Hackers:- The white hat hackers look for bugs and ethically report them to the organization. They are authorized as a user to test for bugs in a website or network and report them to the organization. They generally get all the needed information about the application or network to test for from the organization itself.

* Black Hat Hackers:- The Black hat hackers doesn't allow the user to test through the organization. They unethically enter inside the website and steal data from the admin panel or manipulate the data. They only focus on themselves and the advantages they get from the personal data ~~from~~ for personal financial gain.

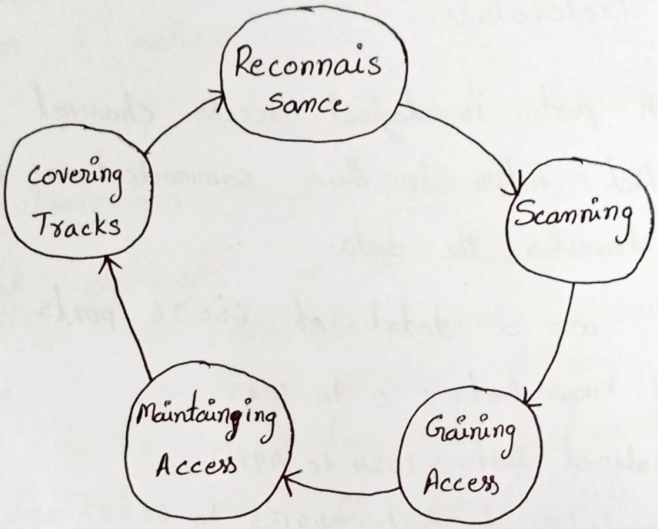
* Grey Hat Hackers:- The Grey Hat Hackers sometimes access to the data and violates the law, But never have the same intention as Black hat hackers, they often operate for the common good. The main difference is that they exploit vulnerabilities publicly where as white hat hackers do it privately for the company.

* Blue Hat Hackers:- The Blue Hat Hackers are much like the script kiddies, are beginners in the field of hacking.

* Green Hat Hackers:- The Green Hat Hackers are also amateurs in the world of hacking but they are bit different from script kiddies. They care about hacking and strive to become full-blown hackers.

* Red Hat Hackers:- Red hat hackers are also known as the eagle-eyed hackers. Like white hat hackers, red hat hackers also aims to halt the black hat hackers. There is a major difference in the way they operate.

→ Phases of Hacking:-



* Reconnaissance :- In this Phase, Attacker find information about Target. It can be done actively or passively. It brings us closer to the target by giving some sensitive information about target.

* Scanning :- In this phase, Attacker find much more information about the ~~target~~ target. Attacker can perform port scanning or various assessments in order to get sensitive information about target.

* Gaining Access :- In this phase, Attacker actually performs HACK. Using the information or vulnerability found by previous phases, attacker takes advantage and perform exploit to gain access.

* Maintaining Access :- In this phase, Attacker installs backdoors or Trojans in order to maintain access into the target system. It is a type of malware to edit & delete the files in victim system.

* Covering Tracks :- In this phase, Attacker deletes the logs and session details in order to not be get caught.

→ Ports and Protocols :-

* Ports :- A port is logical access channel between two devices which helps in their communication. A port is used to transfer the data.

There are a total of 65536 ports i.e., 0 to 65535

1. well known Ports : 0 to 1023
2. Registered Ports : 1024 to 49151
3. Dynamic / Private Ports: 49152 to 65535

Some of the useful ports are :

Port Name	Port Number
ftp	21/tcp
Ssh	22/tcp
telnet	23/tcp
stmp	25/tcp
Http	80/tcp
kerberos	88/tcp
Pop3	110/tcp
Imap	143/tcp
Https	443/tcp
ftps-data	989/tcp
ftps	990/tcp

Telnets	992/tcp
Imaps	993/tcp
pop3s	995/tcp
Ldap	389/tcp.

* Protocols :- Protocol is simply a set of rules which defines a standard way for exchanging information over a network.

Most commonly used protocols are :-

1) Transmission control Protocol (TCP) :- It is one of the main protocols of the Internet Protocol suite. It lies between the application and network layers which are used in providing reliable delivery services. It provides the facility to exchange the information or data directly between two hosts. Ex :- email, file transfer etc.

2) Internet Protocol (IP) :- It is other core part of IPS [Internet Protocol suite]. IP is the main communication protocol which is used for exchanging packets over inter-network using IPS. IP is used to deliver packets from source to destination. It is responsible for establishment of Internet.

3) User Datagram Protocol (UDP) :- It does not contain any flag. In UDP, simple transmission model is used and there is no handshaking methods is used which results into unrealiability, duplication and missing of the information without notice.

→ Primary Network Types :-

1) Local Area Network [LAN] :- In LAN, a computer network cover small local area like home, office and small workgroups such as schools or university. Wi-fi and ethernet are commonly used of LAN.

2) Wide Area Network [WAN] :- In WAN, a computer network cover larger area like on national or regional level. A WAN can be used as LAN, MAN (or) CAN.

3) Wireless Local Area Network [WLAN] :- In WLAN, devices are connected wirelessly by the mechanism of wireless distribution method OFDM Radio [Orthogonal Frequency - Division Multiplexing] or any other.

→ Virtualization :- It is a software technology by which it is possible to run multiple operating systems on the same device or server at the same time. It is one of the efficient way and reduce costs of multiple system setup.

Virtualization is very helpful when you need to demonstrate something between two different os. For Example, A malware target windows machine can be run parallel to the attacker linux machine and it will be much easier to analyze the behavior.

→ Virtualization Software :- Virtualization software are design to run multiple operating systems at the same instant on the same system.

Some of the commonly used virtualization software are :-

1) VmWare Workstation :- Download : http://www.vmware.com/in/products/workstation.

2) Virtual Box :- Download : https://www.virtualbox.org/wiki/Downloads.

* Using Vmware work station :-

1) Download and Install Vmware Workstation.

2) Open VmWare Workstation & click on "create virtual machine".

3) Choose the image file of Operating System or application.

4) Choose the name of operating system or application and select it's version.

5) Provide Hard-drive space for virtual machine and click on finish (min. required : 20 GB)

6) Virtual machine is ready to use. start from the home screen of VmWare Workstation.

→ Kali Linux :- It is a linux based operating system which is a powerful and most popular hacking os itself. It is used to perform penetration testing and vulnerability assessment. It is derived from Backtrack distribution. Kali Linux is developed by offensive security. It contains more than 300 of pre-installed penetration testing scripts and programs. Net Hunter is specially designed for Android Devices. Some of the included tools are as follows:-

* Wireshark
* Metasploit Framework
* Burp Suite
* Kismet
* hping3
* Social Engineering Toolkit
* Armitage
* Nmap
* Aircrack

Some of the supported platforms are as follows:-
Kali linux is available for both 32 bit and 64 bit ARM Architectures. [Advanced RISC Machine].
Kali linux is available for following devices :-

1) BeagleBone Black
2) Hp chrome book
3) Cubie Board2
4) CuBox
5) Raspberry Pi
6) Utilite Pro
7) Galaxy Note 10.1

and rest device can use via Raspberry Pi Image.

→ Installation Requirements :-

* Minimum of 20 GB of hard drive space
* Minimum of 4 GB of RAM
* CD-DVD Drive / USB support.

* Installing Kali Linux as Virtual Machine :-

→ Open VMware & click on create virtual machine

→ Now locate image file of kali linux. Give it name kali and choose UBUNTU as OS Type.
[Note :- UBUNTU is one of the most secure OS around]

→ Give hard drive space for kali linux virtual machine.

→ start kali virtual machine. while booting it will show some options like live (forensics mode) / install / Graphical install.

→ If you want to test kali linux environment than just click on live forensics mode else install it in virtual machine by click on graphical install.

→ Follow these steps for Graphical Install :-

* Choose desire language
* Select country, Tertitary or area
* choose key map (keyboard layout will vary for different key map)
* Configure the Network and setup User Account
* choose Manual partitioning and select the desired partition.
* After that system will install and became ready to use.

(or)

Another way to Install Kali Linux :-

step 1 :- Install your VMware software

step 2 :- Download the kali linux .ISO file and check the image integrity.

step 3 :- Launch your new virtual machine i.e., click on create a New virtual machine.

step 4 :- Installation procedure.

* Once the VM is powered on, you will be prompted to select your preferred installation mode and continue.
* Here we can select live forensics mode.

step 5 :- Disk partitioning

* Once your basic system configuration is set, the installer will ask you to choose a partitioning option for your virtual disk. Choose Guided - Use Entire Disk. for the easiest option.
* select the partitioning disk and hit continue.
* Confirm all the changes that are made to the changes to the disk on the host machine.

Step 6 :- Configure the package manager

* Once the necessary files are installed the installer will ask if you want to set up a Network Mirror.

Step 7 :- Install GRUB boot loader

* Once you have selected your package manager option you will be asked to install the GRUB boot loader. [GRUB : GRand Unified Boot loader]
* Select yes and pick the device to write the necessary boot loader information onto the information to the virtual disk.

Step 8 :- Finished

* Once the installer finishes installing the GRUB to the disk, click on continue to finish the installation process.

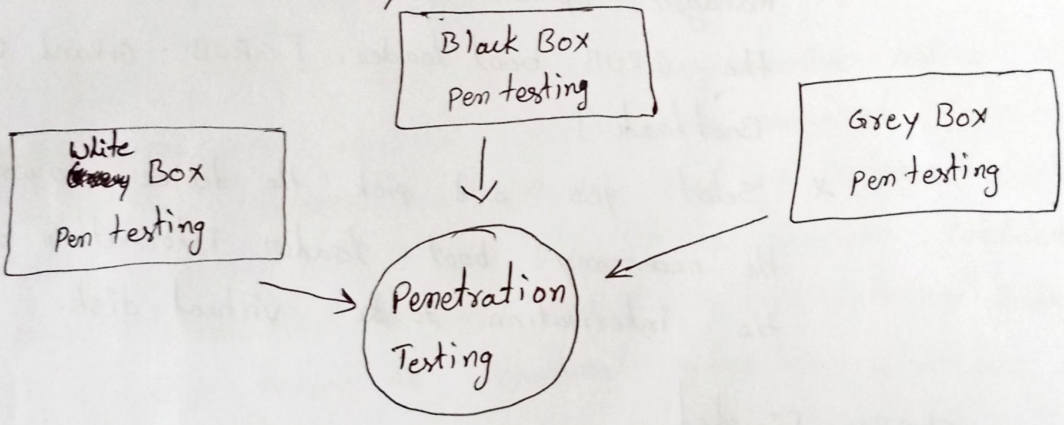
→ Introduction to Penetration Testing :- It is a type of testing to check the security of an application It is to conduct to find the security risk which might be present in the system.

If a system is not secured, then any attacker can disrupt or the take authorized access to that system. Security risk is normally an accidental error that occurs while developing &

implementing the software. Ex: Configuration errors, design errors, and s/w bugs etc.

→ Types of pen testing :-

* Black Box Pentesting
* white Box "
* Grey Box "



* Black Box Penetration testing :- In this testing, tester has no idea about the systems that they are going to test. He is interested to gather information about the target network or system. Ex:- in this testing, a tester only knows what should be the expected outcome and he does not know how the outcome arrives. He does not examine any programming codes.

* Advantages :- 1) Tester need not necessarily be an expert, as it does not demand specific language knowledge.

2) Tester verifies contradictions in the actual System and the specifications.

3) Test is generally conducted with the perspective of a user, not the designer.

* Dis Advantages :- 1) Particularly, these kinds of test cases are difficult to design.

2) Possibly, it is not worth, incase designer has already conducted a test case.

3) It does not conduct everything.

* White box x testing (Penetration) :- This is a comprehensive testing, as tester has been provided with whole range of information about the systems and network such as schema, source code, OS details, IP address, etc. It is normally considered as a simulation of an attack by an internal source. It is also known as structural, glass box, clear box and open box testing.

This testing examines the code coverage and does data flow testing, path testing, loop testing etc.

* Advantages :- 1) It ensures that all independent paths of a module have been exercised.

2) It ensures that all logical decisions have been verified along with their true and false value.

3) It discovers the typographical errors and does syntax checking.

* Dis-Advantages :- 1) Having easy access to information might lead tester in going in an entirely different direction then a hacker would go.

2) It can be a slow process if the tester has to cover a larger amount of data.

* Grey box penetration testing :- In this testing a tester usually provides partial or limited information about the internal details of the program of a system. It can be considered as an attack by an external hacker who had gained illegitimate (by the not authorized law) access to an organization's network infrastructure documents

* Advantages :- 1) As the tester does not require the access of source code, it is non-intrusive and unbiased.

2) As there is clear different between a developer and a tester, so there is least risk of personal conflict.

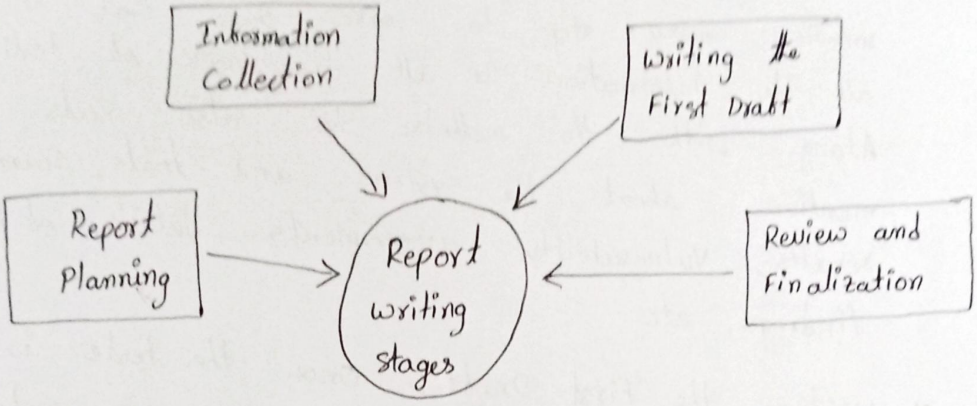
* Dis Advantages :- 1) Testers have no auess to source code and may miss certain critical Vulnerabilitie

2) It is not ideal for algorithm testing.

→ Areas of penetration testing :-

* Network penetration testing
* Application penetration testing
* The response or workflow of the system.

→ Structure of penetration test Report :-



Due to the comprehensive writing work involved, penetration report writing is classified into the following stages :-

* Report Planning
* Information collection
* writing the First Draft
* Review and Finalization

* Report Planning :- It starts with the objectives, which help readers to understand the main points of the penetrating testing. This part describes why the testing is conducted, what are the benefits of pen testing, etc. Secondly, report planning also includes the time taken for the testing.

Major elements of report writing are

* objectives
* time
* Target Audience (managers, security officers)
* Report classification
* Report Distribution

* Information Collection :- Because of the complicated and lengthy processes, pen tester is required to mention every step to make sure that he collected all the information in all the stages of testing. Along with the methods, he also needs to mention about the systems and tools, scanning results, Vulnerability assessments details of his findings, etc.

* Writing the First Draft :- Once the tester is ready with all tools and information, now he needs to start the first draft. Primarily, he needs to write the first draft in the details, mentioning everything i.e., all activities, processes and experiences.

* Review and Finalization :- Once the report is drafted it has to be reviewed first by the drafter himself and then by his seniors or colleagues who may have assisted him. While reviewing, reviewer is expected to check every detail of the report and find any flaw that needs to be corrected.