Unit-2

Notes with reference to question bank topics. 😁

1. Difference between authenticated and unauthenticated penetration testing.

   Ans:

Authenticated Penetration Testing	Unauthenticated Penetration Testing
1. Testing is done using authenticated username and password.	1. Testing is done without using usernames and password.
2. Chance of getting caught is less.	2. Chance of getting caught is high.
3. Low Risk.	3. High Risk.
4. Attacker has a better knowledge of the inside network.	4. Attacker does not has any knowledge about the internal network.
5. Severity is high.	5. Severity is low.

2] Difference between penetration testing and vulnerability assessment.

Ans:

Penetration Testing	Vulnerability Assessment
1. Attempts to actively exploit weakness in an environment.	1. Searches system for known vulnerability.
2. Semi-automated needs human intervention.	2. Can be fully automated.
3. Goal to gain unauthorized access through exploitation.	3. Goal is to scan for loop-holes.
4. Focused on simulating a real-life attack.	4. Focused on in-depth evaluation of a security infrastructure.
5. It is goal oriented.	5. It is list oriented.

3] Difference between internal and external penetration testing. Ans:

Internal Penetration testing	External Penetration testing
1. Consultant is placed within the corporate environment.	1. Consultant looks for security issues from outside the corporate environment.
2. While finding the security issues the consultant is connected to your internal network.	2. While finding the security issues the consultant is connected over the public network.
3. Simulates what an insider can accomplish.	3. Simulates what an outsider can accomplish.
4. Much more devastating.	4. Less devastating in compare to interal testing.
5. The consultant has an authorized access.	5. The consultant does not have an authorized access.
6. The consultant has the knowledge of the internal network.	6. The consultant has no knowledge of the internal network.

4] Difference between black, white and grey hackers. Ans:

Black Hat Hackers	White Hat Hackers	Grey Hat Hackers
1. They are the computer criminals who exploit these vulnerabilities for their personal gain.	1. They are the computer experts they use programming skills to see the vulnerabilities in computer systems.	1. They are also computer experts.
2. They have a motive to earn huge profits.	2. They have genuine license who focuses on penetration testing.	2. They disclose the security flaw to the public.
3. Use their skills for personal gains.	3. Don't use their skills for illegal purposes.	3. Ethical standards fall somewhere between strictly unselfish and strictly malicious.
4. Hack banks, steal credit card personal information, placing malware, etc.	4. They improve the defence for security.	4. Reasons either ethically or unethically depending in the condition and circumstances at hand.
5. Basic strategies are Duplicate content, Invisible text and stuffed keywords, Links from sites with non-relevant content.	5. Basic strategies are Relevant content, Well labeled images, Complete sentences with good spelling and grammar.	5. They use combination strategies of both according to their personal use.

5] Difference between white and black box testing. Ans:

Black Box Testing	White Box Testing
1. It is a software testing method in which the internal structure/design/implementation of the item being tested is not known to the tester.	1. It is a software testing method in which the internal structure/design/implementation of the item being tested is known to the tester
2. Knowledge of Programming language is not required.	2. Deep knowledge of programming language in required.
3. Implementation Knowledge is not required.	3. Implementation knowledge is required.
4. The tester examines the application's external functional behavior and GUI features.	4. The tester has to correct the code also.
5. Done by independent software testers.	5. Done by developers.
6. Requirement specifications is the basis for conducting black box testing.	6. Detail design specifications is the basis for conducting white box testing.

6] Difference between Manual and automated penetration testing. Ans:

Manual Penetration Testing	Automated Penetration Testing
1. It requires expert engineer to perform the test.	1. It is automated so even a learner can run the test.
2. It requires different tools for the testing.	2. It has integrated tools does required anything from outside.
3. In this type of testing, results can vary from test to test.	3. It has fixed results.
4. More time is required for testing.	4. Less time is required for testing.
5. Cannot perform multiple testing at a time.	5. Can perform multiple testing at a time.

7] **What is Scanning? Explain different types of scanning.**

Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network. > Network scanning is used to create a profile of the target organization.

Types of Scanning

1. Port Scanning : To find open ports and services on target
2. Network Scanning: Find IP address in the network of the target
3. Vulnerability Scanning: Find weakness or vulnerabilities on the target

Port Scanning:

In this process the hacker identifies available and open ports and understands what services are running. You must understand the ports and port numbers. The ports numbers can be in these three ranges:

1. Well known Ports from 0 to 1023
2. Registered ports from 1024 to 49151
3. Dynamic Ports from 49152 to 65535

Network Scanning:

- This means to look for active machines or targets on the network.
- This can be done using tools or scripts that ping to all IP addresses on the networks and get a list of the alive nodes and their IP addresses.
- Scans that fit into this category are those such as ping sweeps, which rapidly scan a range of IPs and determine if an address has a powered-on host attached to it or not. > Tools to perform this type of scan include nmap and Angry IP as well as others.

Vulnerability Scanning:

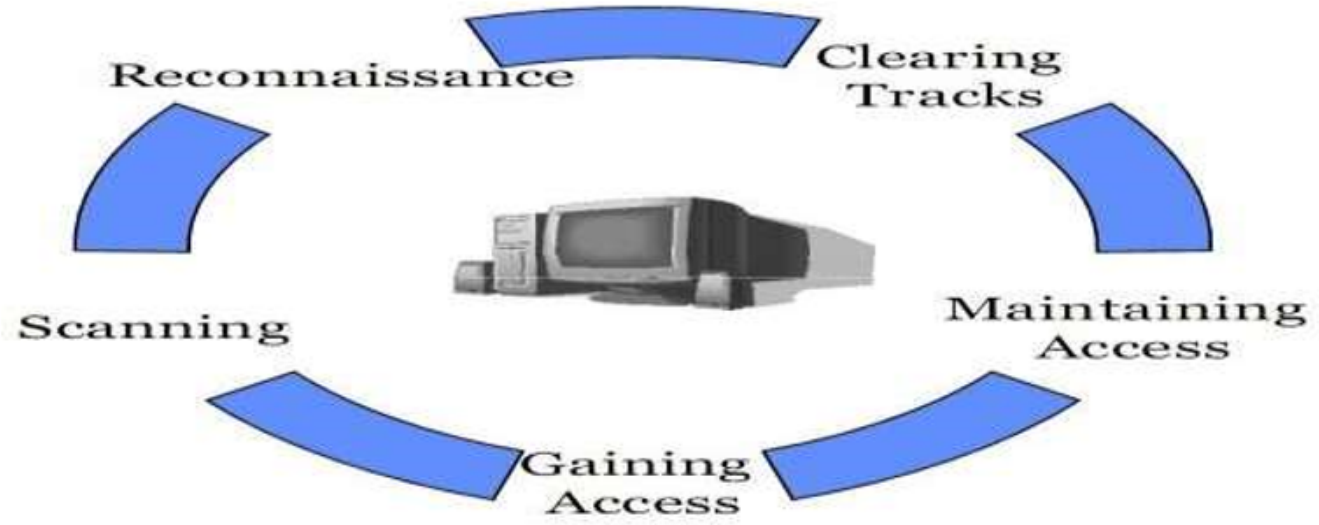
- This is the mechanism where the target is scanned or looked for any vulnerability.
- This type of scan is quite commonly done as a proactive measure, with the goal of catching problems internally before an attacker is able to locate those same vulnerabilities and act on them.
- A typical vulnerability scan will discover hosts, access points, and open ports; analyze service response; classify threats; and generate reports.

8] What is ethical hacking? Why it is important and state how it is different from security auditing. Ans:

An ethical hacker, also referred to as a white hat hacker, is an information security expert who systematically attempts to penetrate a computer system, network, application or other computing resource on behalf of its owners -- and with their permission -- to find security vulnerabilities that a malicious hacker could potentially exploit. Ethical hacking is important as

1. It protects our system from unauthorized access, safeguard the system and information from malicious attack.
2. It is use to test networks at regular interval.
3. It develops preventive measures in order to avoid security breaches. Ethical hacking and Security auditing both are used to keep the important data of a business organization or a security agency safe from the malicious hackers. But in ethical hacking we find the loopholes in the system and in security auditing we use to determine regulatory compliance of the system. So if you see Security auditing as cake, Ethical hacking is a piece of cake.

9] State the phases of hacking.



The Five Phases of Hacking Reconnaissance:- > This is the primary phase where the Hacker tries to collect as much information as possible about the target. > It includes Identifying the Target, finding out the target's IP Address Range, Network, DNS records e.t.c.

Scanning:- > It involves taking the information discovered during reconnaissance and using it to examine the network. > Tools that a hacker may employ during the scanning phase can include dialers, port scanners, network mappers, sweepers, and vulnerability scanners. > Hackers are seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts.

Gaining Access:- > After scanning, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. > This is the phase where the real hacking takes place.

Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. > The method of connection the hacker uses for an exploit can be a local area network (LAN, either wired or wireless), local access to a PC, the Internet, or offline. > Examples include stack based buffer overflows, denial of service (DoS), and session hijacking. > These topics will be discussed in later chapters. Gaining access is known in the hacker world as owning the system.

Maintaining Access:- > Once a hacker has gained access, they want to keep that access for future exploitation and attacks. > Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits, and Trojans. > Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system.

Covering Tracks:- > Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. > Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms. > Examples of activities during this phase of the attack include steganography, the use of tunneling protocols, and altering log files.

10] Working of web inspect and Qualys.

Web inspect tool (crawling/spidering, audit):

1. It is a web application security assessment tool.
2. It is a automated, dynamic web application testing across a web software portfolio.

3. It uses dynamic analysis to show exploitability of web application and web server vulnerabilities.
4. It is a tool used to manage DAST (dynamic application security testing) or DDAST (distributed dynamic application security testing).
5. Web inspect is a application, scanning tool provided by hp.
6. It helps the security professionals to assess security flaws in web application.
7. It is a dynamic black box testing tool.

Step 1) Installation Step 2) Perform crawling/spidering Step 3) Perform audit

Crawling: It is a process of building tree structure for a website by traversing every possible links on that site.

Audit: It is a process of performing attacks to access the vulnerabilities.

Working with web inspect: -

https://dl.packetstormsecurity.net/papers/attack/WebInspect.pdf

Qualys:-

1. It is scan tool for vulnerability management
2. It is a commercial network-based application used to collect information about the target without running an actual vulnerability scanning
3. It can be used to proactively locate, identify and assess vulnerabilities to prioritized and correct before they are targeted and exploited by attackers

Working with Qualys https://community.qualys.com/docs/DOC-3848

It's easy to launch a vulnerability scan, and there's just a few simple steps. Your scan results will show you the vulnerabilities discovered in your network.

Step 1: Add IP Addresses to Scan Go to Assets > Host Assets to see the IP addresses available to you. If the IPs you want to scan are not listed then you have to add them (or have your manager add them and assign them to you).

Step 2: Scan Option Profiles You'll need an option profile at scan time. The option profile defines the scan settings you want to use. Several profiles are provided to get you started. You can use these profiles as-is or fine tune the scan settings and then save them for future use. Go to Scans > Option Profiles to see the profiles available to you. Create a new profile from the New menu or edit a profile in the list.

Step 3: Start Your Scan You're now ready to start your first vulnerability scan! Go to Scans > Scans and choose New > Scan.

Provide a title, select an option profile and select target hosts to scan. For your first scan, it's recommended you limit the scan to a small number of IP addresses. The service will perform external scanning unless you have appliances in your account and choose one. When you're ready, click Launch.

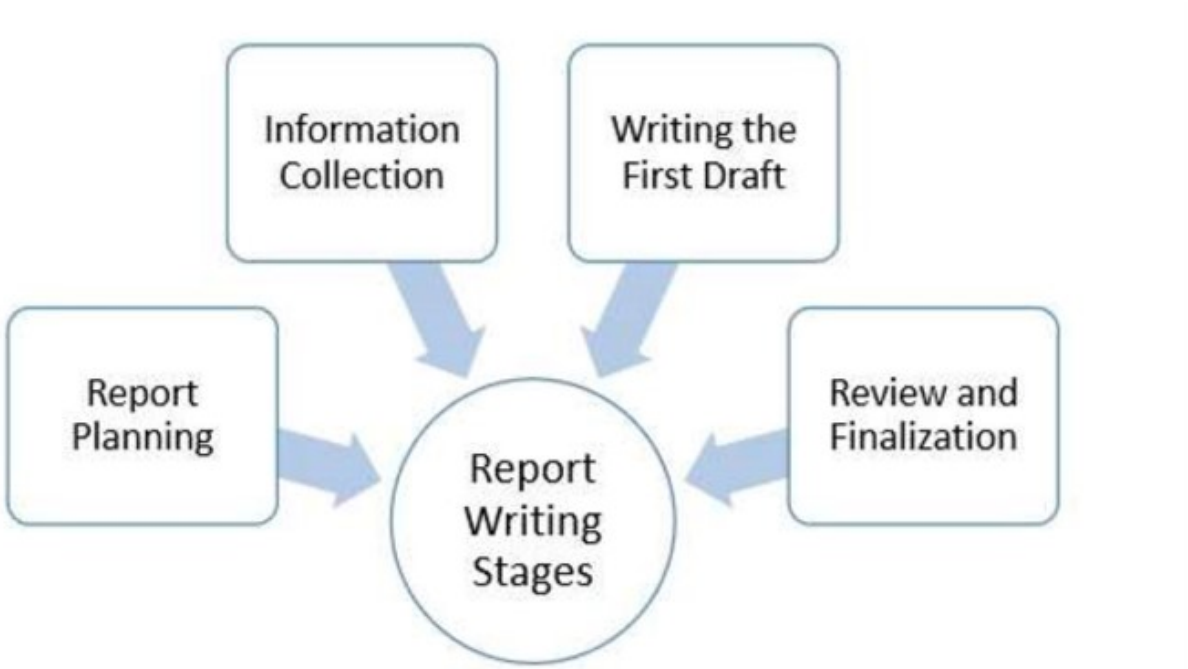
Step 4: View Scan Status and Results The scan status window appears as soon as your scan starts. The status is updated every 60 seconds until all targeted hosts have been analyzed. You can safely close this window and let the scan run in the background. You can return to the scan status window from the scans list at any time to get the latest information about your scan.

When the scan is finished check out the Scanners section. You can expand details to see which scanners were used to scan the hosts. Click the View Results button to see the full scan results. (Note that the Scanners section is only visible in accounts with New Scanner Services enabled.)

11] Write a short note for report preparation for penetration testing. Ans:

In penetration testing, report writing is a comprehensive task that includes methodology, procedures, proper explanation of report content and design, detailed example of testing report, and tester's personal experience.
Once the report is prepared, it is shared among the senior management staff and technical team of target organizations.
If any such kind of need arises in future, this report is used as the reference. Penetration report writing is classified into the following stages −

1. Report Planning
2. Information Collection
3. Writing the First Draft
4. Review and Finalization



Report Planning

Report planning starts with the objectives, which help readers to understand the main points of the penetration testing.
This part describes why the testing is conducted, what are the benefits of pen testing, etc.

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.

12] Explain the contents of a report. Ans: Following is the typical content of a penetration testing report –

1. Executive Summary
    - Scope of work
    - Project objectives
    - Assumption
    - Timeline
    - Summary of findings
    - Summary of recommendation
2. Methodology
    - Planning
    - Exploitation
    - Reporting
3. Detail Findings
    - Detailed systems information
    - Windows server information

References Appendix