UNIT II

CHAPTER 2

Ethical Hacking - I (Introduction & Pre-Attack)

Syllabus Topics

Introduction : Black Hat vs. Gray Hat vs. White Hat (Ethical) hacking, Why is Ethical hacking needed?, How is Ethical hacking different from security auditing and digital forensics?, Signing NDA, Compliance and Regulatory concerns, Black box vs. White box vs. Black box, Vulnerability assessment and Penetration Testing.

Approach : Planning - Threat Modeling, set up security verification standards, Set up security testing plan – When, which systems/apps, understanding functionality, black/gray/white, authenticated vs. unauthenticated, internal vs. external PT, Information gathering, Perform Manual and automated (Tools: WebInspect/Qualys, Nessus, Proxies, Metasploit) VA and PT, How WebInspect/Qualys tools work: Crawling/Spidering, requests forging, pattern matching to known vulnerability database and Analyzing results, Preparing report, Fixing security gaps following the report

Enterprise strategy : Repeated PT, approval by security testing team, Continuous Application Security Testing,

Phases : Reconnaissance/foot-printing/Enumeration, **Phases**: Scanning, Sniffing

Syllabus Topic : Ethical Hacking

2.1 Introduction

GQ. 2.1.1 Define the term:
a. Hacking b. Ethical Hacking

Hacking

- Hacking is very broad discipline that covers a wide range of topics, which has been a part of computing for last five decades.
- In 1960 at MIT, the first event of hacking had taken place and on that event the term "Hacker" was originated.
- It is the act of finding possible entry points that exist in a computer system or a network and finally entering into them.
- Hacking is basically used to gain unauthorized access to a computer system or a computer network which either to harm the systems or to steal sensitive information available on the computer.

Ethical Hacking

- Ethical hacking involves an authorized attempt to gain unauthorized access to a data or computer system.
- It is also known as White hat Hacking.
- It is usually legal only when it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is which called as **Ethical Hacking**.
- It is used to improve the security of the systems and networks by fixing the vulnerability found while testing.

Types of Hacking

- We can categorize hacking based on what being hacked, so the following are the types:
  1. Network Hacking
  2. Website Hacking
  3. Computer Hacking
  4. Password Hacking
  5. Email Hacking

Syllabus Topic : Black Hat vs. Grey Hat vs. White Hat (Ethical) hacking

2.1.1 Black Hat vs. Grey Hat vs White Hat

GQ. 2.1.2 Define Hacker. Enlist Type of Hacker. Explain its types in details.

GQ. 2.1.3 What is difference between Black Hat vs. Gray Hat vs. White Hat.

Hacker

- Hacker is a computer expert who does the act of hacking.
- Hackers are those who try to obtain knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems.
- He improves the security posture of an organization.
- Ethical hackers use the same tricks, tools, and techniques that malicious hackers used, but with the permission of the authorized person.
- The main purpose of ethical hacking is to improve the security and to defend the systems from attacks by malicious users.

Hackers are classified into three categories

1. Black Hat Hacker

- Black Hat hackers also known as crackers.
- They hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.
- Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, damaging the system, violating privacy, blocking network communication, etc.

2. White Hat Hacker

- White Hat hackers are also known as **Ethical Hackers.**
- They never intent to harm a system, instead they try to find out weaknesses in a computer or a network system as part of penetration testing and vulnerability assessments.
- Ethical hacking is not illegal, is one of the demanding jobs available in the IT industry.
- There are many companies that hire ethical hackers for penetration testing and vulnerability assessments.

3. Grey Hat Hacker

- Grey hat hackers are a blend of both white hat and black hat hackers.
- They act without malicious intent but for their fun, they utilize a security weakness in a computer system or computer network without the owner's permission or knowledge.
- Their intention is to bring weakness to the attention of the owners and getting appreciation or little reward from the owners.

Syllabus Topic : Ethical Hacking Needed?

2.1.2 Ethical hacking needed?

GQ. 2.1.4 Why Ethical Hacking needed?

- Ethical hacking now days is used as a common and favoured process to analyze the security systems and programs of an organization.
- It runs parallel with red teaming security judgment, intrusion testing, and vulnerability.
- Some important points that will help us understand more about ethical hacking and its necessity.
  - o While hacking a computer system an ethical hacker usually tends to play the role of a security expert. They penetrate into system in order to detect risks and illegal access of the system. They constantly have to face two obstacles: threat and vulnerability.
  - o Ethical hacking follows guidelines of safe hacking for the efficient working of the system. It is a complex procedure hence an ethical hacker requires great skills in comparison to penetration testing.
  - o To fight against unlawful practices of breaching systems and to take precautionary actions on hackers, Ethical Hacking comes handy in corporate sectors and organizations.
  - o Dangerous software like viruses, Trojan horses, and spam email causes disruption and disturbance in the system and storage space. Ethical hacking provides useful here as it helps to uncover such virus attacks against systems and in addition provides high-level security.
  - o The main objective of ethical hacking is to **promise safety** in wireless infrastructure which constitutes most of current business companies aims.

- Ethical hacking has privilege of gathering access to a company's network and information system. It automatically provides security to intellectual attacks and threats like viruses. Ethical hacking as a result ends up also testing the security levels of the programs and software.

Syllabus Topic : How is Ethical hacking different from security auditing and digital forensics?

2.1.3 How is Ethical Hacking Different from Security Auditing and Digital Forensics?

GQ. 2.1.5 How is Ethical hacking different from security auditing?

Many people confuse ethical hacking with security auditing, but there are big differences. Security auditing involves comparing a company's security policies to what's actually taking place.

Security Auditing

- The intention of security auditing is to validate that security controls exist, typically using a risk-based approach.
- Security auditing involves reviewing business processes and in many cases, it might not be very technical.
- Not all Security audits are this high-level, but majority is quite simplistic.

Ethical Hacking

- It focuses on vulnerabilities that can be exploited.
- This Hacking validates that security controls do not exist or are ineffectual at best. It can be both highly technical and nontechnical and although you can use a formal methodology which tends to be a bit less structured than formal auditing.
- If auditing continues take place in your organization, you might consider integrating ethical hacking techniques into your IT audit program. They both are complement one another really well.

Syllabus Topic : Signing NDA

2.1.4 Signing NDA

GQ. 2.1.6 What is NDA? Explain the things before to signing NDA.

UQ. 2.1.7 Define the term NDA. (MU - April-18)

- A Non-Disclosure Agreement (NDA) is a written document establishing a legally binding, confidential relationship between parties, providing what information parties consider confidential, and prohibition of the other party from revealing it to others.
- A patron will often require an employee to sign an NDA because it allows their company to operate at a higher level with less risk.
- A functional NDA is catalyst for free flow of confidential information within company, pivotal for maximizing profit and efficiency, without fear of such information being made publicly available.
- Confidential and proprietary information that companies aim to keep secret includes technologies, client lists, proprietary relationships, marketing and design strategies, and various other trade secrets.
- Your employer is not asking you to sign an NDA out of mistrust but they asking you to sign one because it is essential to conducting business smoothly and efficiently.

Seven Things Should Consider Before Signing

1. Look for broad and vague language

- When analyzing NDA, make sure that the definitions of proprietary and confidential information are thoroughly defined.
- Be dubious of broad and vague language that optimizes to unreasonably limit your ability to discuss and divulge information.
- In order to better protect yourself make sure to exclude these four categories of information from your NDA :
  - Publicly available information
  - Information you already possess or may acquire on your own
  - Information you can prove you learned of independent of protected information provided for under the NDA
  - Information received by a third party source

2. Understand the document's scope

- Reflect on what NDA is asking you to keep confidential and for how long.
  - What must you do to keep the information secret?
  - What type of information is you prohibited from disclosing?
  - How long after your departure are you expected to keep the information private?

3. The consequences of breaching it

- Be careful of unusually extreme or unfair punishments for breaching the NDA.
- Consider proportionality of the punishment to the breach, and if punishment far outweighs the breach, abstain from signing.
- Make sure the NDA isn't heavily in favor of one party.
- Steer clear of an NDA that foist responsibility on you for breaches by third parties which including your co-workers and other employees without similar provision to balance.

4. The timing of your John Hancock

- Consider a bargained for exchange of value between parties, It is a basic element of all contracts.
- It will likely be asked to sign your NDA at before you start work, where your employment is sufficient as standalone consideration.
- This issue arises once you are asked to sign an NDA after starting your job. You may be entitled to fresh consideration.
- After commencing work, an employee is asked to sign an NDA as your states are new and fresh.
- As you are fresh consideration may come in the form of a promotion, a bonus, additional vacation days, or various other employee benefits.

5. Liquidated damages

- Run, and don't look back. Without ever having to prove you were the direct cause , an NDA containing a liquidated damages provision entitles your employer to a specified amount of damages paid to them,.
- Most liquidated damages provisions are contrary and oppressive to public policy.

- *Don't handout your employer an automatic recovery for something you may not have even done.*

6. You can negotiate

- Don't be afraid to ask to modify or alter documents terms if you think something is unfair or out of place.
- It never hurts to ask and companies are much more likely to allow changes to surprise or last-minute NDAs.
- There should be a balance between parties with any functional contract.
- Ask for clarifications, and spell out any concerns you have about provisions or terms of the agreement.

7. Go with your gut

- If something in NDA seems suspicious, you seem like an inconvenience having a lower check over your contract and NDA, but it is a fraction of cost and bother you could suffer later on down the road.
- A few amounts now could save you years of hardship, stress, and even a lawsuit.
- There is nothing wrong with scrapping the NDA altogether and walking away, if the NDA seems overly oppressive or suspicious,.
- NDA are essential for any employer looking to protect their proprietary and confidential information.

Syllabus Topic : Compliance and Regulatory Concerns

2.1.5 Compliance and Regulatory Concerns

GQ. 2.1.8 Write a short note on compliance and Regulatory concerns.

- Compliance regulations often address security and privacy together as well as laying down directives to safeguard a company's IT systems and its data from cyber-attacks.
- These regulations put ,a responsibility on companies to protect themselves from accidental breaches.
- Data regulations also cover paper records in similar manner to digital records.
- Companies can undertake several actions to protect their systems and their information, including anti-virus software, firewalls, data encryption and IDS With respect to online and networked data.
- It is essential to give training to employees to use the company's cyber security structures.
- These actions start a company on its journey towards compliance taken together.
- Well-known regulations include the U.S. Federal Information Security Management Act (FISMA), and Europe's Directive on Security of Network and Information Systems (the NIS Directive).
- These regulations contain overarching directives and guidelines and are relevant for nearly all companies handling data.
- The Payment Card Industry Data Security Standard (PCI DSS) addresses issues related to the use of credit cards in online and offline environments similarly.

Syllabus Topic : Black box vs. White box vs. Black box

2.1.6 Black box vs. White box

GQ. 2.1.9 Give difference between Black box vs White Box

Sr. No	Black Box	White Box
1	Black Box is a way of software testing in which the internal structure or the program or the code is hidden and nothing is known about it.	White Box is a way of testing the software in which the tester has knowledge about the internal structure or the code or the program of the software.
2	Mostly done by software testers.	Mostly done by software developers.
3	No knowledge of implementation is needed.	Knowledge of implementation is required.
4	Referred as outer or external software testing.	The inner or the internal software testing.
5	It is functional test of software.	It is structural test of software.
6	No knowledge of programming is required.	Mandatory to have knowledge of programming.
7	It is the behaviour testing of software.	It is the logic testing of software.
8	It is applicable to the higher levels of testing of software.	It is generally applicable to the lower levels of software testing.
9	It is also called closed testing.	It is also called as clear box testing.
10	**Example :** search something on Google by using keywords	**Example :** by input to check and verify loops
11	Types of Black Box Testing : – Functional Testing, – Non-functional testing, – Regression Testing	Types of White Box Testing : – Path Testing, – Loop Testing, – Condition testing

Syllabus Topic : Vulnerability assessment and Penetration Testing

2.1.7 Vulnerability Assessment and Penetration Testing

UQ. 2.1.10 Define the Term :
a. Penetration Testing
b. Vulnerability Testing (MU - April 18)

GQ. 2.1.11 Give Difference between Penetration Testing and Vulnerability Testing.

Penetration Testing

- Penetration testing replicates the actions of an internalor/ and external cyber attackers that is intended to break the information security and hack the valuable data or interrupt the normal functioning of the organization.
- A penetration tester (ethical hacker) makes an effort to control critical systems and acquire access to sensitive data with the help of advanced tools and techniques.

Vulnerability Assessment

- A vulnerability assessment is the technique of identifying and measuring security vulnerabilities in a given environment.
- It is a comprehensive assessment of the information security position (Result Analysis).
- It identifies the potential weaknesses and provides proper mitigation measures to either remove those weaknesses or reduce below the risk level.
- The following diagram summarizes the vulnerability assessment

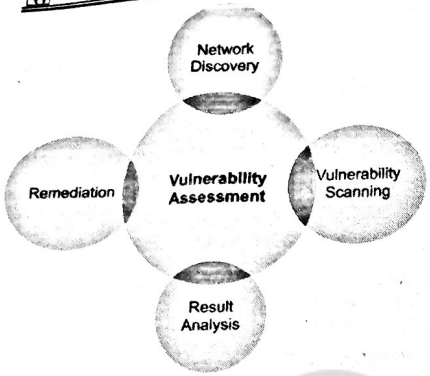


Fig 2.1.1 : Vulnerability Assessment

Sr. No	Penetration Testing	Vulnerability Assessments
1	It determines the scope of an attack.	It makes a directory of assets and resources in a given system.
2	It tests sensitive data collection.	It discovers the potential threats to each resource.
3	It gathers targeted information and/or inspects the system.	It allocates quantifiable value and significance to the available resources.
4	It cleans up the system and gives final report.	It attempts to mitigate or eliminate the potential vulnerabilities of valuable resources.
5	Non-intrusive, documentation and environmental review and analysis.	It is Comprehensive analysis and through review of the target system and its environment.
6	Ideal for physical environments and network architecture.	Ideal for lab environments.
7	Meant for critical real-time systems.	Meant for non-critical systems.

Syllabus Topic : Approach - Planning / Threat Modelling

2.2 Approach - Planning / Threat Modelling

GQ. 2.2.1 Explain the term Thread Modelling.

- It can be done at any stage of development but if done at the beginning it will help in early determination of threats that can be distributed properly.
- The purpose of Threat modelling is to identify, communicate, and understand threats and alleviation to the organization's stakeholders as early as possible.
- Documentation from this process provide system analyst and defenders with a complete analysis of probable attackers profile, the most likely attack vectors, and the assets most desired by the attacker.

Threat modelling helps to achieve following

1. It defines security of application
2. It Identifies and investigates potential threats and vulnerabilities
3. Its results in finding architecture bugs earlier

There is various threat modelling methodologies available:

1. Strike

- It is a methodology developed by Microsoft for threat modelling.
- It provides a mnemonic for security threats in six categories :
  1. **Spoofing :** An adversary posing as another user, component, or other system that has an identity in system being modelled.
  2. **Tampering :** Modification of data within the system to achieve malicious goal.

3. **Repudiation :** Ability of an adversary to deny performing some malicious activity in absence of sufficient proof.
4. **Information Disclosure :** Exposure of protected data to a user that is not otherwise allowed access to that data.
5. **Denial of Service :** It Occurs when an adversary uses illegitimate means to assume a trust level than he currently has with different privileges.

2. DFD

- It is the input of this approach and each node of the DFD is applied to the system.
- The possible number of security threats will be identified, as well as feasible mitigation.

3. DREAD

- It was proposed for threat modelling but due to inconsistent ratings it was dropped by Microsoft in 2008
- DREAD is currently used by OpenStack and many other corporations.
- It provides a mnemonic for risk rating security threats using five categories.
- The categories are :
  1. **Damage Potential :** It ranks the extent of damage that would occur if vulnerability is exploited.
  2. **Reproducibility :** It ranks how easy it is to reproduce an attack
  3. **Exploitability :** It assigns a number to the effort required to launch the attack.
  4. **Affected Users :** A value characterizing how many people will be impacted if an exploit become widely available.
  5. **Discoverability :** It measures the likelihood how easy it is to discover the threat.

The risk can be calculated in DREAD model by taking average of 5 categories:

Risk = (Damage Potential Reproducibility +Exploitability Affected Users +Discoverability)/5

4. P.A.S.T.A.

- The Process for Attack Simulation and Threat Analysis (PASTA) is a seven step risk-centric methodology.
- The purpose is to provide a dynamic threat identification, enumeration, and scoring process.
- Upon completion of threat model security subject matter experts develop a detailed analysis of the identified threats.
- Finally, appropriate security controls can be enumerated which helps developer to develop a asset-centric mitigation strategy by analysing attacker-centric view of application.

5. Trike

- Its focus is in using threat models as risk management tool.
- Threat models are based on requirement model, so the requirements model establishes the stakeholder defined acceptable level of risk assigned to each asset class.
- Analysis of requirements model yields a threat model from which threats are identified and assigned risk values.
- The completed threat model is used to build risk model on the basis of asset, roles, actions, and calculated risk exposure.

6. VAST

- VAST is Stands for Visual, Agile, and Simple Threat modelling.

- The methodology provides actionable outputs for unique needs of various stakeholders like developers, application architects and cyber security personnel etc.
- VAST provides a unique application and infrastructure visualisation scheme such that the creation and use of threat models do not require specific security subject matter expertise.

Syllabus Topic : Set up Security Verification Standards

2.2.2 Set up Security Verification Standards

GQ. 2.2.2 Write a short note on Security verification standards.

- The OWASP Application Security Verification Standard (ASVS) Project is providing a basis for testing web application technical security controls.
- It also provides developers with a list of requirements for secure development.
- The primary aim of the OWASP ASVS Project is to normalize the range in the coverage and level of rigor available in the market when it comes to performing Web application security verification using commercially workable open standard.
- The standard provides a basis for testing application technical security controls and any technical security controls in the environment that are relied on to protect against vulnerabilities such as XSS and SQL injection.
- It can be used to establish a level of confidence in the security of Web applications.
- The requirements were developed with the following objectives in mind :

1. **Use as a metric :** It Provide application developers and application owners with a yardstick with which to assess the degree of trust that can be placed in their Web applications,
2. **Use as guidance :** It Provide guidance to security control developers as to what to build into security controls in order to satisfy application security requirements.
3. **Use during procurement :** It Provide a basis for specifying application security verification requirements in contracts.

Syllabus Topic : Set up Security Testing Plan - When, Which Systems / apps

2.2.3 Set up Security Testing Plan – When, Which Systems / apps

UQ. 2.2.3 Write a short note on Security Testing plan. (MU - April 2018)

- Security Testing is defined as a type of Software Testing that ensures software systems and applications are free from any vulnerability, risks, threats that may cause a big loss.
- Security testing of any system is about finding all possible loopholes and weaknesses of system which might result into loss of information, revenue, repute at the hands of the employees or outsiders of the Organization.
- Its goal is to identify the threats in the system and measure its potential vulnerabilities, so system does not stop functioning or is exploited.
- It also helps in detecting all possible security risks in system and help developers in fixing these problems through coding.

Types of Security Testing

- There are seven types of security testing as per Open Source Security Testing methodology manual :

1. Vulnerability Scanning
2. Security Scanning
3. Penetration testing
4. Risk Assessment
5. Security Auditing
6. Ethical hacking
7. Posture Assessment

1. **Vulnerability Scanning :** It is done through automated software to scan a system against known vulnerability signatures.
2. **Security Scanning :** Security Scanning involves identifying network and system weaknesses and later provides solutions for reducing these risks. This scanning can be performed for both Manual scanning and Automated scanning.
3. **Penetration testing :** This is kind of testing simulates an attack from a malicious hacker. PT involves analysis of a particular system to check for potential vulnerabilities to an external hacking attempt.
4. **Risk Assessment:** It involves analysis of security risks observed in the organization. Risks are classified as Low, Medium and High. It recommends controls and measures to reduce the risk.
5. **Security Auditing :** It is an internal inspection of Applications and OS for security flaws.
6. **Ethical hacking :** It is hacking Organization Software systems. It's intention is to expose security flaws in the system.
7. **Posture Assessment :** It combines Security scanning, Ethical Hacking and Risk Assessments to show an overall security posture of an organization.

Syllabus Topic : Understanding Functionality, Black/ Grey/ White

2.2.4 Understanding Functionality, Black/ Grey/ White

UQ. 2.2.4 Explain Black, Grey and White Box penetration Testing methods in details. (MU - April 2018)

- The type of penetration testing normally depends on the scope and the organizational requirements and wants.
- It is also known as Pen Testing.

Types of Penetration Testing

- Following are the important types of pen testing
  1. Black Box Penetration Testing
  2. White Box Penetration Testing
  3. Grey Box Penetration Testing

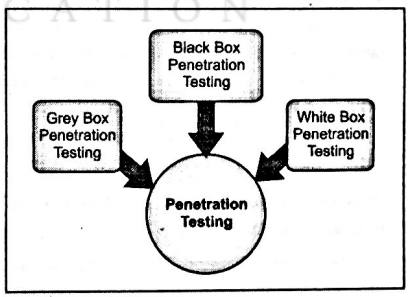


Fig 2.2.1 : Penetration Testing

1. Black Box Penetration Testing

- Tester has no idea about the systems that he is going to test in black box penetration testing,.

- Tester is interested to gather information about the target network or system.
- For example, in this testing a tester only know what should be the expected outcome and he does not know how the outcomes arrive.
- Tester does not examine any programming codes.

☞ **Advantages of Black Box Penetration Testing**

- Tester need not be an expert, as it does not demand knowledge about specific language
- Tester verifies contradiction in the actual system and the specifications
- Test is generally conducted with the user perspective not the designer

☞ **Disadvantages of Black Box Penetration Testing**

- These kinds of test cases are difficult to design.
- This Testing is not worth, incase designer has already conducted a test case.
- Black Box Testing does not conduct everything.

2. White Box Penetration Testing

- White Box Penetration Testing is a complete testing as tester has been provided with entire range of information about the systems and network such as Source code, Schema, OS details, IP address, etc.
- It is considered as a simulation of an attack by an internal source.
- It is also known as structural, glass box, open box, and clear box testing.
- This testing examines the code coverage and does data flow testing, path testing, loop testing, etc.

☞ **Advantages of White Box Penetration Testing**

- Ensures that all independent paths of a module have been exercised.
- Ensures that all logical decisions have been verified along with their true and false value.
- Discovers the typographical errors and does syntax checking.
- Finds the design errors that may have occurred because of the difference between logical flow of the program and the actual execution.

3. Grey Box Penetration Testing

- A tester usually provides partial or limited information about the internal details of the program of a system in Grey Box Penetration testing.
- It considered as an attack by an external hacker who had gained illegal access to an organizations network infrastructure documents.

☞ **Advantages of Grey Box Penetration Testing**

- It is non-intrusive and unbiased as the tester does not require the access of source code.
- There is least risk of personal conflict as there is clear difference between a developer and a tester.
- Not need to provide the internal information about the program functions and other operations.

Syllabus Topic : Authenticated vs. Unauthenticated

2.2.5 Authenticated vs. Unauthenticated

GQ. 2.2.5 Give Difference between authenticated vs unauthenticated.

☞ **Unauthenticated Penetration Testing**

- It is an examination of an asset without login credentials usually a username and password.
- It simulates how a random outside attacker would approach the asset.

- It involves examining the security perimeter of an asset without any login credentials or access rights.
- An Unauthenticated Penetration Test may suffice if your goal is to satisfy certain compliance standards that require regular perimeter testing.
- Gain awareness of vulnerabilities, such as open ports in firewalls, that attacker used to breach your perimeter defenses.
- It can highlight perimeter security gaps, it has its own limitations.
- Remember,

No access credentials = Unauthenticated

☞ **Authenticated Penetration Testing**

- It is an examination of an asset from the perspective of an attacker who has managed to gain entry, whether with compromised login credentials, or a malicious employee with access rights.
- It involves examining an asset with login credentials or access rights in order to determine how much maneuverability someone has once inside.
- Shearwater recommends you undergo an Authenticated Penetration Test as for a more complete picture of what damage an intruder could do once they're on the inside.
- Conducting this Testing offers deeper awareness into potential risks from a broader range of vulnerabilities.
- Remember,

Access credentials = Authenticated

Syllabus Topic : Internal vs. External PT

2.2.6 Internal vs. External PT

GQ. 2.2.6 Give Difference between Internal and external Penetration Testing.

☞ **External Penetration Testing**

- It refers to assets that are externally facing.
- Assets are usually accessible via the internet.
- Some examples may include email, websites, or file sharing platforms.

☞ **Internal Penetration Testing**

- It refers to assets that are internally facing.
- Accessible from within an organizational environment
- For example, a network or a server.
- Depending on whether you have access credentials both External and Internal assets can be tested in an Unauthenticated or an Authenticated way.

Syllabus Topic : Information Gathering

2.2.7 Information Gathering

GQ. 2.2.7 Write a short note on Information Gathering.

- Information gathering is also known as foot printing an organization.
- It begins by determining the target system, application, or physical location of the target.
- Once this information is known then specific information about the organization is gathered using nonintrusive methods.
- For example, the organizations own web page may provide a personnel directory or a list of employee bios which may prove useful if the hacker needs to use a social engineering attack to reach the objective.
- Information gathering can be broken into seven logical steps :

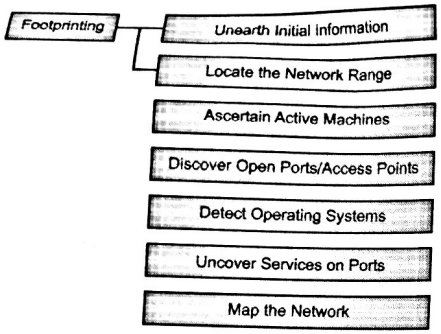


Fig 2.2.2 : Seven steps of Information Gathering

- This process is performed during the first two steps of unearthing initial information and locating the network range.
- Some of the common sources used for information gathering include the following:
  1. Domain name lookup
  2. Whois
  3. Nslookup
  4. Sam Spade

Syllabus Topic : Perform Manual and Automated (Tools : WebInspect/ Qualys, Nessus, Metasploit) VA and PT

2.2.8 Perform Manual and Automated (Tools : WebInspect/ Qualys, Nessus, Proxies, Metasploit) VA and PT

GQ. 2.2.8 How to perform Manual Penetration Testing.

GQ. 2.2.9 Define Automated penetration Testing. Explain its various tools.

GQ. 2.2.10 Give the difference between Manual and Automated Penetration Testing.

Manual penetration testing

It is the testing that is done by human beings. In this testing vulnerability and risk of a machine is tested by an expert engineer. Testing engineers perform the following methods :

- **Data Collection** - It plays a key role for testing. One can either collect data manually or can use tool services freely available online. These tools help to collect information like DB versions, database ,table names, software, hardware, or even about different third party plugins, etc
- **Vulnerability Assessment** - It helps the testers to identify the security weakness and take preventive steps accordingly once the data is collected.
- **Actual Exploit** - It is a typical method that an expert tester uses to launch an attack on a target system and likewise to reduces the risk of attack.
- **Report Preparation** - The tester prepares a final report that describes everything about the system once the penetration Testing is done. Finally report is analyzed to take corrective steps to protect the target system.

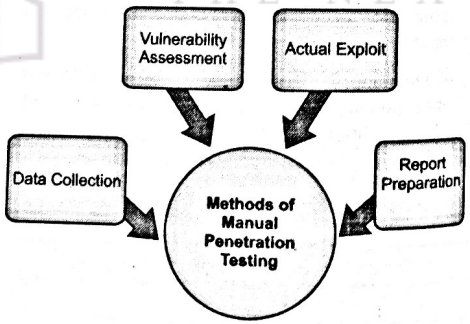


Fig 2.2.3 : Manual Penetration Testing

Manual penetration testing is categorized in two following ways

Focused Manual Penetration Testing

1. It is much focused method that tests specific vulnerabilities and risks.
2. It is only done by human experts who examine specific application vulnerabilities within the given domains.
   - Comprehensive Manual Penetration Testing –
   - It is through testing of whole system connected with each other to identify all sorts of risk and vulnerability.
   - The function of this testing is more situational such as investigating whether multiple lower-risk faults can bring more vulnerable attack scenario, etc.

☞ Automated penetration testing

- It is much faster, easy, efficient, and reliable that tests the vulnerability and risk of a machine automatically.
- This technology does not require any expert engineer; rather it can be run by any person having least knowledge of this field.
- Tools for automated penetration testing are Nessus, OpenVAs, Metasploit, backtract (series 5), etc.
- These are very efficient tools that changed the efficiency and meaning of penetration testing.

☞ Tools

1. Nessus

- Nessus is freeware network vulnerability scanner which has more than 11,000 plug-ins available.
- It includes a client - server architecture with a GTK graphical interface, remote and local security checks and an embedded scripting language for writing own plug-ins or understanding existing ones.

2. QualysGuard

- QualysGuard is a web-based vulnerability scanner. Users can securely access this tool through an easy-to-use web interface.
- It features more than 5,000 vulnerability checks as well as an inference-based scanning engine.

3. Metasploit Framework

- This is an open-source software product used to test, develop, and use exploit code.
- Difference between Manual Penetrations Testing vs. Automated Penetration Testing

Sr. No	Manual Penetration Testing	Automated Penetration Testing
1	Requires expert engineer to perform the test.	a learner can run test because it is automated
2	Requires different tools for the testing.	It has integrated tools, use if does required anything from outside.
3	Results can vary from test to test.	It has fixed result.
4	Requires remembering cleaning up memory by the tester.	It does not.
5	Exhaustive and time taking.	More efficient and fast.
6	An expert can run multiple testing as per the requirement,.	It cannot.
7	It is more reliable for critical condition.	It is not.

Syllabus Topic : How WebInspect / Qualys tools work

2.2.9 How WebInspect/Qualys tools work

GQ. 2.2.11 Explain Working of WebInspect tool.

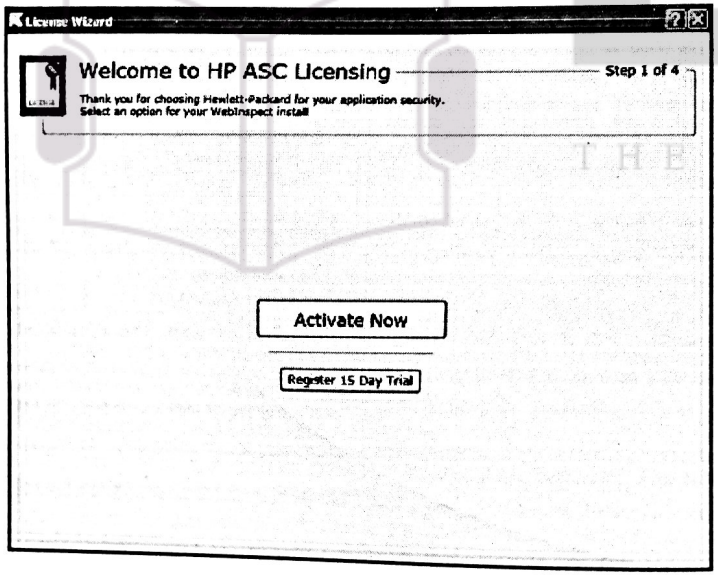
GQ. 2.2.12 Explain Working of Qualys tool.

WebInspect

- *WebInspect is a web application security scanning tool introduced by HP.*
- It helps the security professionals to assess the potential security flaws in web application.
- It is basically a dynamic black box testing tool which detects the vulnerabilities by actually performing the attack.
- There are assessment agents that work on different areas of the application after initiating the scan on the web application.
- They report their results to security engine which evaluate the results.
- It uses Audit engines to attack the application and determine the vulnerabilities.
- At the end of the scan you can generate a report called Vulnerability Assessment Report which would list the security issues in desired format.
- Using this report, client can fix the issues and then go for validation scanning to confirm the same.
- HP WebInspect is a commercial tool and you need license to scan a web site.

Installation of WebInspect

- Requirement before install WebInspect:
- 2 GB RAM
- Microsoft SQL Server installed
- After installation the first time you start WebInspect it will open the 'License Wizard' and prompt you to activate by entering the license key.
- If you don't have one, you can go for a 15 day trial period for which activation token will be sent to your mail after giving details



- Two things that WebInspect will do for you: Crawl and Audit

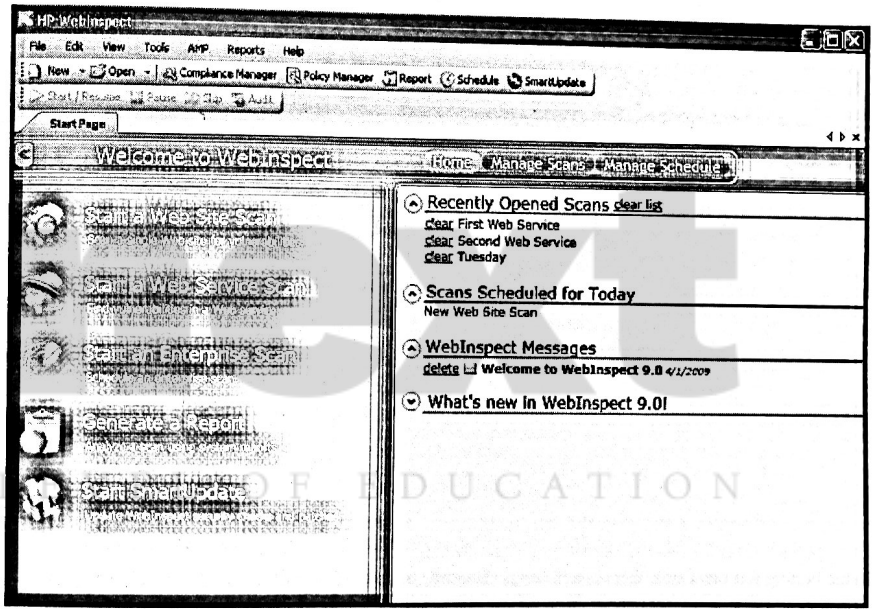
1. **Crawl :** It is a process by which WebInspect will build the tree structure of the entire website by traversing every possible link on that site.
2. **Audit :** It is the process of performing attacks to assess the vulnerabilities.

Scan= Crawl + Audit

Two things that you need to do for WebInspect: Configure and Analyze.

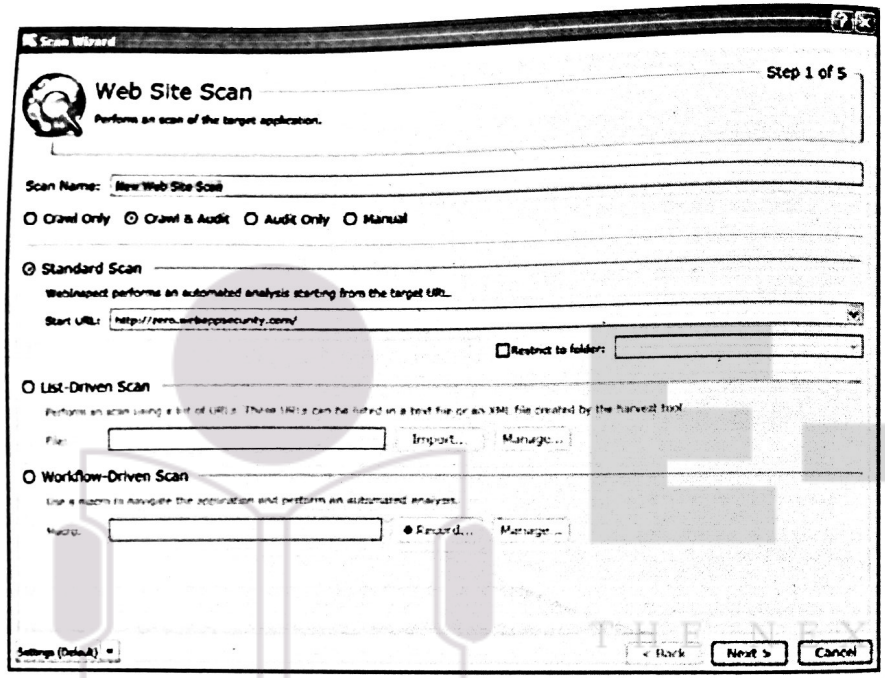
Starting a Scan :

Step1 : Start WebInspect and click File-->New

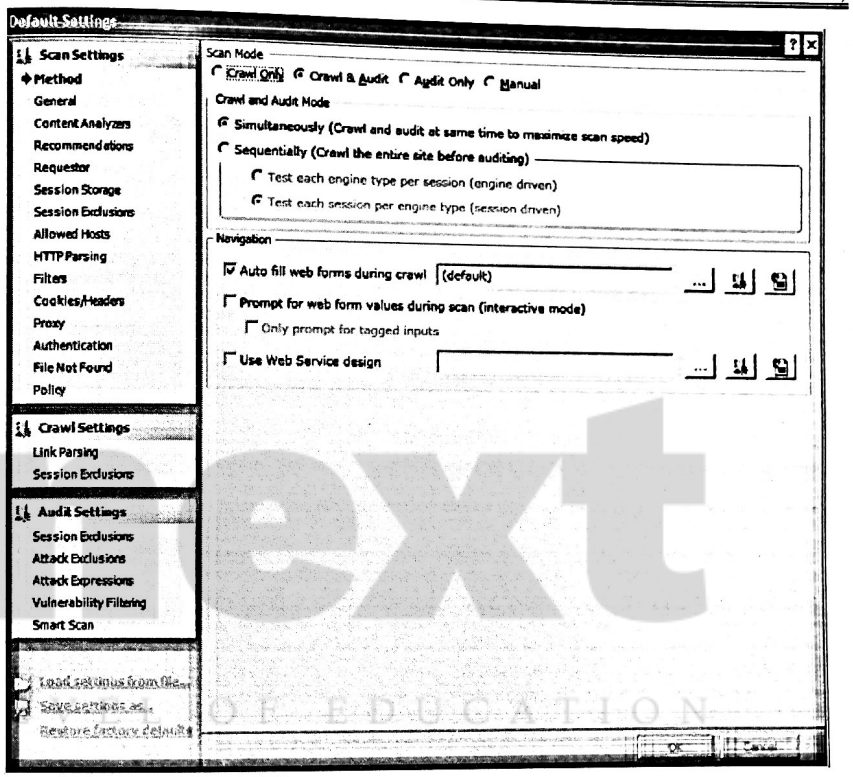


- As you can see in the above picture 'Scan Wizard' opens and you can select the type of scan you want to conduct. So select 'Website scan'. In scan wizard on the right hand side you can see the recently opened scans and the scans that are in schedule. We can schedule a scan to begin at a particular time.

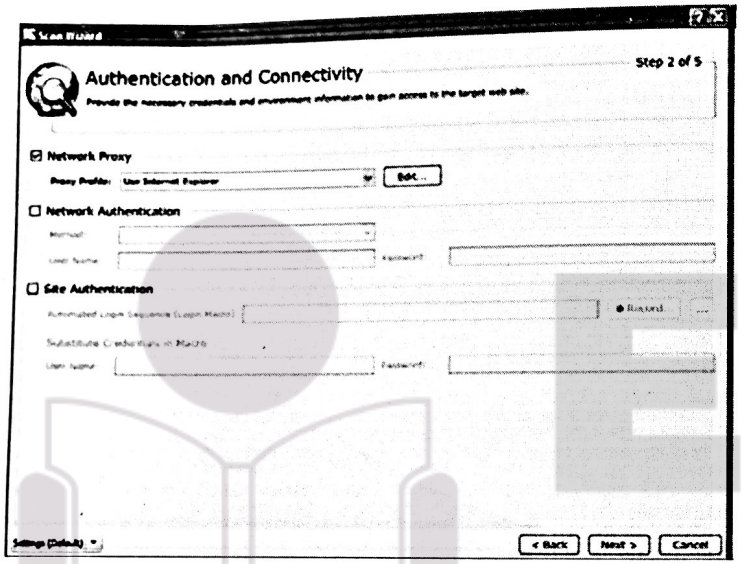
- **Step 2 :** Upon selecting Website scan you will be taken to the below window where you need to enter scan name. Select crawl and audit button and select the type of Scan (Standard Scan, List-Driven Scan, Window-Driven Scan, Manual Scan).



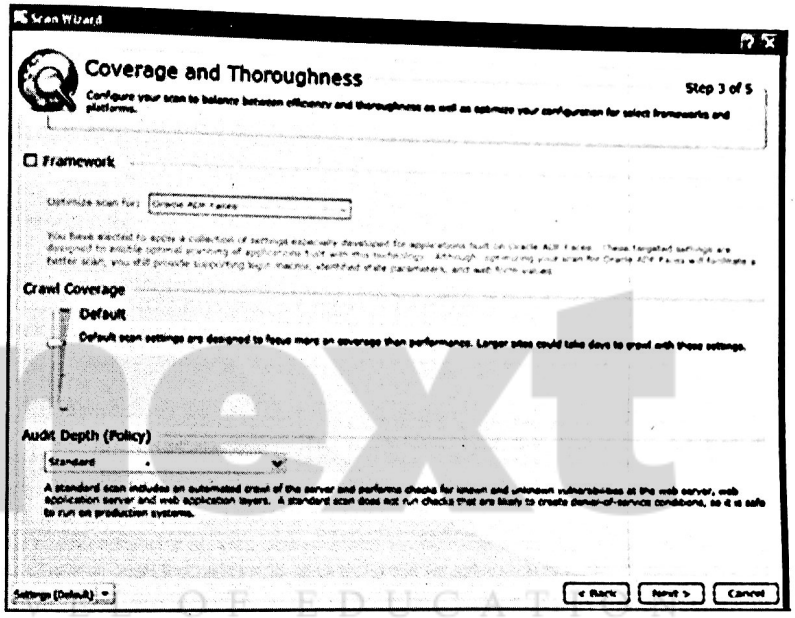
- In the bottom left hand side, there is a **Settings (Default)** button which is the heart of WebInspect.
- Using this you configure the scan and tell WebInspect what you want from it. Click on Settings (Default) and 'Default Settings' window will open.



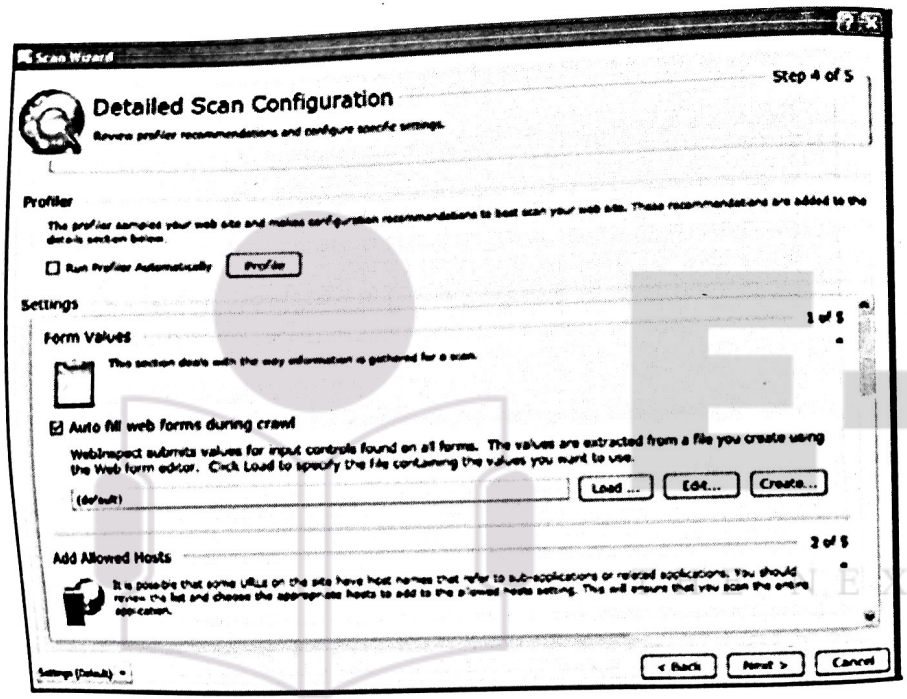
- **Step 3 :** Once you are done with the Default settings click on next and Authentication and Connectivity window appears below figure. Here values are shown based on your input under proxy tab and authentication tab in Default Settings window.



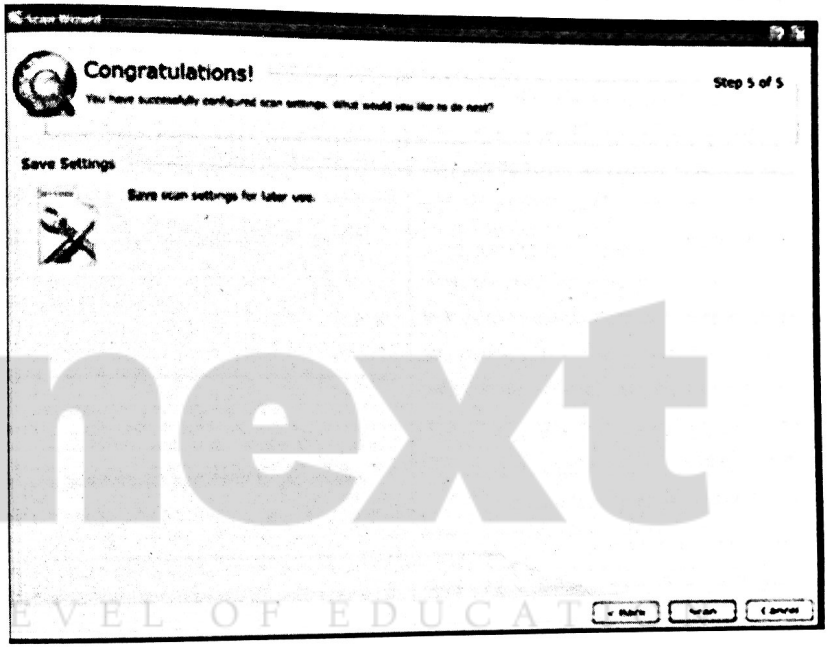
- **Step 4 :** Click to next, new window **Coverage and thoroughness** appear where information about crawl coverage and audit depth will be shown based on your input under requester tab in default setting.



▶ **Step 5 :** Click on next Detailed scan configuration window appears. Under this profiler runs a quick examination of the target and if necessary it recommend you certain changes. You may or may not accept the recommendation.



▶ **Step 6 :** Move to next window where you can find the 'scan' button. Scan will initiate once clicking the scan button. The scan completion time depends on size of the application, selected policy and other factors.



▶ **Step 7 :** Once the scan gets completed, need to analyze the result to eliminate the false positives and generate report for valid findings.

It must be clear that the Default scan settings play crucial role in optimizing the results.

☞ Advantages

1. It is save time when dealing with large enterprise applications.
2. It simulates the attack, shows results and presents you with a comprehensive view.
3. Not dependent on the underlying language.

☞ Disadvantages

1. It is hard for any tool to find logical flaws, weak cryptographic storage, severity of the disclosed information etc.
2. There could be false positives among listed vulnerabilities.

Qualys Tool

Working with Qualys Tool

Create a Qualys user account with the role of Manager or Unit Manger. Make sure that you have your account information.

1. Open browser and go to the platform URL where your account is located. Please refer to your registration email containing your platform URL and login credentials. A Manager or Unit Manager account is required.
2. On the Qualys LOGIN page, enter your user name (login) and password, and then click LOGIN. You are prompted to review and accept the licensing agreement when you log into your account for the first time. Your Qualys Home page appears upon successful login.
3. Select VM from the application picker.
4. Go to Scans > Appliances.
5. Select New > Scanner Appliance and enter activation code for the appliance (as it appears in the ACTIVATION CODE screen in your Appliance's user interface.

Note : The activation code is shown only when Appliance has not been activated yet.

6. Select an asset group that you want to add the Scanner Appliance (Unit Manager only) from the Add to menu. This will make the Appliance available to users in business unit.
7. Click Activate. Then Scanner Appliance attempts to log in to the Qualys Cloud Platform.

Note : It may take few minutes for Scanner Appliance activation to occur. Complete activation manually by restarting the Scanner Appliance if you prefer not to wait,. Just press the Down arrow until SYSTEM REBOOT screen appears and then press ENTER. When REALLY REBOOT SYSTEM? appear press ENTER.

8. The Scanner Appliance Name–IP Address message appears after Scanner Appliance makes a successful login to the Qualys Cloud Platform. Do you see another message instead? See Troubleshooting and we'll help you with this.

Syllabus Topic : Crawling / Spidering

2.2.10 Crawling / Spidering

UQ. 2.2.13 Write a short Note on Crawling with Example. (MU - April 2018)

- Spammers and anyone else interested in collecting e-mail addresses from Internet can use web spiders.
- A web spider separate websites collecting certain information such as email addresses.
- The web spider uses syntax such as the @ symbol to locate email addresses then copies them into list.
- These addresses are then added to a database and may be used later to send unrequested e-mails.
- They can be used to locate all kinds of information on the Internet.

- A hacker can use the web spider to automate the information gathering process.
- To prevent web spidering of your website is to put the robots.txt file in the root of your website with a listing of directories that you want to protect from crawling.

Syllabus Topic : Requests forging

2.2.11 Requests Forging

UQ. 2.2.14 Explain Cross-Site Request Forgery. (MU - April 2018)

- The Cross-Site Request Forgery (CSRF) is a hacker that forces an user to execute unwanted actions on a web application in which they are currently authenticated.
- This hacker specifically target only state-changing requests, not theft of data.
- Since the hacker has no way to see the response to the fake request.
- With a little help of social engineering (like sending a link via email or message), ahacker may trick the users of a web application into executing actions of the hacker's choosing.
- If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests such as changing their email address, transferring funds, and so on.
- If the victim is an administrative account, cross site request forgery can compromise the entire web application.

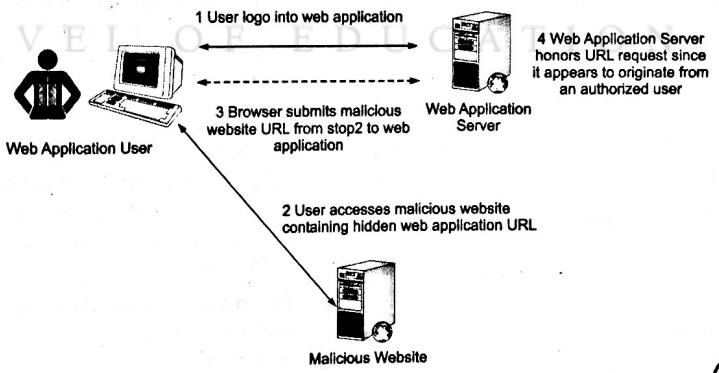


Fig. 2.2.4 : Cross site request forgery

Syllabus Topic : Pattern Matching to known Vulnerability Database and Analysing Results

2.2.12 Pattern Matching to known Vulnerability Database and Analysing Results

An overview of the threat analysis method using the vulnerability DB is shown in Fig.2.1.1

Syllabus Topic : Preparing report

2.2.13 Preparing report

GQ. 2.2.15 Explain how to prepare Penetration Testing Report.

☞ Penetration Testing Report Writing

- Report writing in penetration testing is broader task that includes procedures, methodology, proper explanation of report content and design, detailed example of testing report, and tester personal experience.
- Once report is prepared, it is shared among technical team of target organizations and the senior management staff. If any similar kind of need arises in future, this report is used as the reference.

☞ Report Writing Stages

Penetration Testing report writing is classified into the following stages :

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

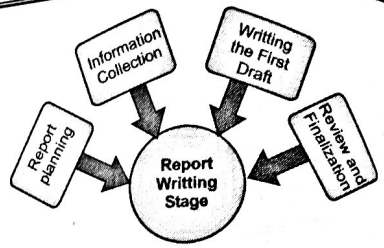


Fig. 2.2.5 : Penetration Testing Report Writing

1. Report Planning

- It starts with the objectives, which help readers to understand main points of the penetration testing.
- In this stage, describes why the testing is conducted, what the benefits of pen testing, etc. It also includes the time taken for the testing.
- Major elements of report writing are –
  - o **Objectives** : It describes overall purpose and benefits of pen testing.
  - o **Time** : Time gives the accurate status of the system so inclusion of time is very important, this report will save the tester if anything wrong happens later as the report will illustrate the risks and vulnerabilities in the penetration testing scope during specific period of time.
  - o **Target Audience** : This testing also needs to include target audience, such as information technology manager, information security manager, chief information security officer, and technical team.
  - o **Report Classification** : This report is highly confidential which carry server IP addresses, application information, threats, vulnerability; it needs to be classified properly. But this classification needs to be done on the basis of target organization which has an information classification policy.

  - o **Report Distribution** : The scope of work should be mentioned number of copies and report distribution. It also needs to mention that hardcopies can be controlled by printing a limited number of copies attached with its number and the receiver's name.

2. Information Collection

- Pen tester is required to mention every step to make sure that he collected all the information in all the stages of testing because of the complicated and lengthy processes.
- He also needs to mention about the systems and tools, vulnerability assessments, scanning results, details of his findings, etc. along with the methods.

3. Writing the First Draft

- Once the tester is ready with all tools and information, he needs to start the first draft.
- Firstly, he needs to write the first draft in the details mentioning everything i.e. all activities, processes, and experiences.

4. Review and Finalization

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

Content of Penetration Testing Report

The typical content of a penetration testing report as follows

☞ Executive Summary

- Scope of work
- Project objectives
- Assumption
- Timeline
- Summary of findings
- Summary of recommendation

☞ Methodology

- Planning
- Exploitation
- Reporting

☞ Detail Findings

- Detailed systems information
- Windows server information

☞ References

- Appendix

Syllabus Topic : Fixing Security gaps Following the Report

2.2.14 Fixing Security gaps Following the Report

The following list of benefits should wholly sell you on the importance of penetration testing :

☞ Real-world experience

- The experience gained in penetration testing can prove invaluable when responding to a real-life security incident.
- In that regard, it's very similar to the tests you conduct to assess your firm's level of disaster preparedness.
- The results will say a lot about the overall effectiveness of your security policies and just how equipped your staff is to handle a breach.

☞ Seal security holes

- A thorough penetration test will uncover any existing weaknesses or flawed staff practices in your infrastructure that could lead to security breaches.

- Your team can use the findings to seal those gaps and strengthen your security prowess.

☞ Improve business continuity

- The more downtime your business experiences, the greater impact it has your on operations and bottom line.
- A proper pen test can highlight potential threats to business continuity and in turn, help ensure the maximum uptime.

☞ Maintain compliance

- Penetration testing is actually a legal requirement in some industries. For instance, the Payment Card Industry Data Security Standard (PCI-DSS) calls for merchants to undergo this process on a regular basis to protect consumer data.
- Making sure these tests are properly conducted will help an organization avoid the hefty penalties that result from failing to meet regulatory compliance.

☞ Tighten up other business areas

- The results of a penetration test can help an organization fine-tune their efforts in areas beyond security.
- A developer can learn exactly how a hacker breached their application and more importantly, make improvements that prevent similar incidents from occurring in the future.

☞ Complement enterprise security

- Penetration testing is a potent security tool in the hands of any business.
- When combined with your security policies, patch management scheduling, threat intelligence processes and other existing security practices, it can play an integral role in rounding out your defences.

☞ Strengthen trust and loyalty

- A successful cyber attack or security breach is almost certain to compromise the trust of your customers, vendors, and business partners. This is especially the case when they are directly affected.
- A company that commits to a regimen of penetration tests and other security assessments can reassure these stakeholders that their confidential information and transactions are secure.

Syllabus Topic : Enterprise Strategy

2.2.15 Enterprise Strategy

1. Define Your Test Goals

- When you establish your goals beforehand, you will have a testing process designed around meeting those objectives.
- So if there is something in particular you want addressed, make sure it is clearly defined when passing your goals along to the testing team.
- Outlining a specific set of goals can help provide the focus needed to determine where your greatest security risks lie.

2. Assemble the Best Team

- The most cost effective route is to assemble a pen testing team from on-staff security personnel. Others enlist the services of a third-party firm.
- The advantage of going outside is having the diligence of specialized professionals who are less likely to take any shortcuts.
- Whether you build from within or bring a specialist aboard, it's critical to understand that the personnel you select can make or break your pen test initiatives.
- You need a team of security experts who can design a comprehensive testing regimen from plan to implementation to reporting content.

3. Think Like a Hacker

- The key to effective penetration testing is thinking and acting like a real-life attacker. Testers must arm themselves with the tools needed to simulate an attack and determine what could happen if a hacker is successful.
- But not all attackers are created equal, so it makes sense to create unique profiles for the most likely intruders.
- It could be a disgruntled ex-employee bent on revenge, or an outsider with little knowledge of the operation. Pen testers should work closely with management and IT to develop profiles that mimic attackers who pose the most realistic threat.

4. Add a Social Component

- Based on sheer prevalence, social engineering should be a major cog in every penetration testing strategy.
- This manipulative technique views employees as the weakest link in your defense system. It entails trying to gain access by tailgating employees.
- The alarming effectiveness of social engineering can be seen in spear phishing. Research shows that spear phishing accounts for more than 90 percent of all cyber attacks and is responsible for the loss of billions of dollars worldwide.
- In addition to popular techniques such as phishing, pen testers should familiarize themselves with the psychology leveraged in social engineering.
- Reciprocation, authority, and scarcity are just some of the motivators social engineers use to trick people into dangerous actions. The closer pen testers come to mimicking social engineering, the better they'll be at revealing an organization's true weaknesses.
- From there they can recommend security mechanisms and educational practices that minimize the risks.

5. Explore All Possible Angles

- There's more than one way to the treasure, and attackers will exploit as many entry points to the company. Ideally, a pen test will target every relevant attack vector.
- The goal is striking pay dirt by any means necessary. The login data in your printer may seem trivial, but it might share credentials with databases that house customer information, credit card numbers, or other sensitive data.
- When it comes to attack vectors, penetration testing must leave no stone unturned.

6. Let the Data Be Your Guide

- Following a successful cyber security breach, most investigative efforts can be traced to a targeted data set.
- In the process of thinking like an attacker, testers need to identify the data at risk, determine where it resides, and figure out how a real criminal could possibly get their hands on it.
- Be it intellectual property, customer data, or business plans, hawking the most sensitive data will always lead pen testers in the right direction.

7. Choose Your Pen Test Wisely

- While there are several types to choose from, penetration testing is mainly classified in two categories: blackbox and whitebox.
- In a whitebox scenario, the tester has intimate knowledge of, or access to the test subject. Due to the up close and personal nature, this type of test is ideal for internal applications or inside threats.
- In a blackbox scenario, the tester has no knowledge of the test subject. The tester needs to identify any vulnerabilities that come about due to information that is publicly available.
- Since it simulates external attacks, blackboxing is the traditional form of penetration testing.

- There are advantages and disadvantages to each penetration testing strategy. The method you choose is vital to ensuring that the time, budget, and manpower you allocate produces an outcome that aligns with your objectives.

Syllabus Topic : Repeated PT

2.2.16 Repeated PT

- Remediation is an act of offering an improvement to replace a mistake and set it right. Often the presence of vulnerability in one area may indicate weakness in process or development practices that could have replicated or enabled similar vulnerability in other locations.
- Therefore, while remediating, it is important for the tester to carefully investigate the tested entity or applications with ineffective security controls in mind.
- Because of these reasons, the respective company should take steps to remediate any exploitable vulnerability within a reasonable period of time after the original penetration test.
- In fact, as soon as the company has completed these steps, the pen tester should perform a retest to validate the newly implemented controls which are capable to mitigate the original risk.
- The remediation efforts extending for a longer period after the initial pen test possibly require performing a new testing engagement to ensure accurate results of the most current environment.
- This determination should be made after a risk analysis of how much change has occurred since the original testing was completed.
- Moreover, in specific conditions, the flagged security problem may illustrate a basic flaw in respective environment or application.
- Therefore, the scope of a retest should consider whether any changes caused by remediation identified from the test are classified as significant. All changes should be retested; however, whether an entire system retest is necessary or not will be determined by the risk assessment of the changes.

Syllabus Topic : Approval by Security Testing Team

2.2.17 Approval by Security Testing Team

- The key tenets of performing the penetration test on an organization are to get clear and unambiguous permission to conduct test.
- While getting sponsorship and such to perform the test is important, it's essential to document permission.
- Gets the person authorizing a test to formally sign off on the project and the plan, and in case have their contact information on hand.
- The test can run into one of many snags, including that a test was never authorized, which could easily lead to lawsuit against you as the pentester without such authorization.
- So Verbal authorization is not desirable but documentation showing that authorization was granted is acceptable.
- A test should never proceed with only verbal authorization. If you are an outside contractor, a signed contract is enough to convey and enforce permission for action.
- Internal tests can be justified with signed paperwork, an email, or both. It would be unwise and possibly illegal to proceed without this paperwork or permission in place.

- The permission not only gives you authorization to conduct a test but also serves as your "Get out of jail free" card if you are challenged as to whether you should be testing or not.
- Don't ever underestimate importance of having permission to do a test as well as having it in writing.
- Charges have been filed and successfully pursued against those who have not had such documentation or permission.

Syllabus Topic : Continuous Application Security Testing

2.2.18 Continuous Application Security Testing

- Application Security Testing (AST): This form of test focuses specifically on locating and identifying the nature of defects in software applications.
- It can be performed as an independent test or as part of complete testing suite. This process may be requested in those situations where custom applications or environments exist and a closer survey is required.
- The major motivation for using AST tools is that manual code reviews and traditional test plans are time consuming, and new vulnerabilities are continually being introduced or discovered.
- There are many benefits to use this tool which increase the speed, efficiency, and coverage paths for testing applications.
- The tests they conduct are repeatable and scale well once a test case is developed in a tool and can be executed against many lines of code with little incremental cost.
- Application security Testing puts a primary focus on three elements:
  1. It reduce security vulnerabilities and risks
  2. It improving security features and functions such as encryption, authentication or auditing
  3. It integrate with the enterprise security infrastructure
- The Followings are types of Application Security tools :

1. **Static Application Security Testing (SAST)**

- These tools can be thought of as white-box testing, where a tester knows information about the system or software being tested, including an architecture diagram, access to source code, etc.
- It examines source code to detect and report weaknesses that can lead to security vulnerabilities

2. **Dynamic Application Security Testing (DAST)**

- These tools can be thought of as black-box testing, where a tester has no prior knowledge of the system.
- They discover conditions that indicate security vulnerability in an application in its running state.
- DAST tools run on operating code to detect issues with interfaces, requests, responses, data injection, scripting, sessions, authentication, and more.

Syllabus Topic : Phases

2.3 Phases

- An ethical hacker is follows processes similar to those of a malicious hacker.
- The steps to gain and maintain entry into a computer system are similar no matter what the hackers intentions are.

- Below figure illustrates the five phases that hackers generally follow in hacking a system. The following sections cover these five phases.

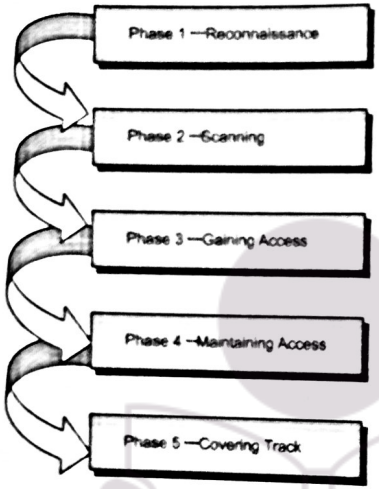


Fig 2.3.1 : Phases of Hacking

There are five phases of Hacking as follows

- Phase 1: Passive and Active Reconnaissance
- Phase 2: Scanning
- Phase 3: Gaining Access
- Phase 4: Maintaining Access
- Phase 5: Covering Tracks

Syllabus Topic : Reconnaissance/ Footprinting / Enumeration

2.3.1 Reconnaissance/ Foot printing/ Enumeration

Reconnaissance

There are two kind of reconnaissance : Passive and Active

1. Passive reconnaissance

- It involves gathering information regarding the potential target without targeted individuals or company's knowledge.
- It can be as simple as watching a building to identify what time employees enter the building and when they leave.
- But it is usually done using Internet searches or by Googling an individual or company to gain information.
- This process is generally called information gathering.
- Social engineering and dumpster diving are also considered passive information-gathering methods. passive reconnaissance means Sniffing the network which can yield useful information such as naming conventions, IP address ranges, hidden servers or networks, and other available services on the system or network.
- Sniffing network traffic is means to building monitoring: A hacker watches flow of data to see what time certain transactions take place and where this traffic is going.

2. Active reconnaissance

- It involves probing the network to discover individual hosts, IP addresses, and services on the network.
- Active reconnaissance usually involves more risk of detection than passive reconnaissance and is also called rattling the doorknobs.
- It can give a hacker an indication of security measures in place but a process also increases the chance of being caught or at least raising suspicion.
- Both passive reconnaissance and active reconnaissance can lead to the discovery of useful information to use in an attack.

- For example, it is usually easy to find the type of web server and the operating system version number that a company is using.
- This information may enable the hacker to find vulnerability in that OS version and utilize the vulnerability to gain more access.

3. Foot Printing

- Footprinting is defined as a process of creating a blueprint or map of systems and an organizations network.
- footprinting an organization is also known as information gathering.
- It begins by determining target system, application, or physical location of the target.
- Once this information is known specific information about organization is gathered using nonintrusive methods.
- For example:
- Organizations own web page may provide a personnel directory or list of employee bios, which may prove useful if the hacker needs to use a social engineering attack to reach objective.
- A hacker may also do a Google search .People search to locate information about employees. The search engine of Google can be used in creative way to perform information gathering.
- To retrieve information has been termed Google hacking use of the Google search engine. http://groups.google.com can be used to search the Google newsgroups.
- The following commands can be used to have the Google search engine perform Google hacking: site searches a specific website or domain. The website to search must be provided after the colon.
- File type searches only within the text of a particular type of file. It must be supplied after the colon.
- Don't include a period before the file extension

4. Enumeration

- It occurs after scanning and is a process of gathering and compiling usernames, network resources, machine names, shares, and services.
- Enumeration also refers to actively querying or connecting to the target system to acquire this information.
- The objective of enumeration is to identify the user account or system account for potential use in hacking the target system.
- It isn't necessary to find a system administrator account, because most account privileges can be escalated to allow an account more access than was previously granted.
- To locate NetBIOS name information, many hacking tools are designed for scanning IP networks.
- For each responding host, the tools list IP address, logged in username, NetBIOS computer name, and MAC address information.
- The built-in tool net view can be used for NetBIOS enumeration on a Windows 2000 domain.
- To enumerates NetBIOS names using a net view command, enter the following at the command prompt :

```
net view / domain nbtstat -A IP address
```

- DumpSec is a NetBIOS enumeration tool.

- This tool connects to the target system as a null user with the net use command. It then enumerates users, NTFS permissions, groups, and file ownership information.

Syllabus Topic : Phases - Scanning

2.3.2 Scanning

- It involves taking the information discovered during reconnaissance and using it to examine the network.
- Tools that a hacker may hire during the scanning phase can include port scanners, dialers, network mappers, sweepers, and vulnerability scanners.
- Hackers are seeking any information that can help them perpetrate attack such as IP addresses, computer names, and user accounts.
- The hacker continues to gather information regarding the network and its individual host systems during scanning.
- Data such as IP addresses, OS, services, and installed applications can help the hacker decide which type of exploit to use in hacking a system.
- It is the process of locating systems that are alive and responding on the network.
- Ethical hackers use it to identify target systems' IP addresses.
- Scanning is performed after the active and passive reconnaissance stages of system hacking have been completed.
- It is used to determine whether a system is on the network and available.
- Scanning tools are used to gather information about a system such as the operating system, IP addresses, and services running on the target computer.

Types of Scanning

1. **Port scanning** : It determines open ports and services
2. **Network scanning** : IP addresses
3. **Vulnerability scanning** : It presence of known weaknesses

1. Port scanning

- It is the process of identifying open and available TCP/IP ports on a system.
- Port scanning tools enable a hacker to learn about services available on a given system.
- Each service or application on the machine is associated with a well-known port number.
- For example, this tool identifies port 80 as open indicates a web server is running on that system. Hackers need to be familiar with port numbers.

2. Network scanning

- It is a procedure for identifying active hosts on a network, either to attack them or as a network security assessment.
- Hosts are identified by their individual IP addresses.
- This tools attempt to identify all a live or responding hosts on the network and their corresponding IP addresses.

3. Vulnerability scanning

- It is the process of proactively identifying the vulnerabilities of computer systems on a network. It first identifies the OS and version number, including service packs that may be installed.
- Then, the vulnerability scanner identifies weaknesses or vulnerabilities in the OS.
- During the later attack phase, a hacker can utilize those weaknesses in order to gain access to the system.

Syllabus Topic : Phases - Sniffing

2.3.3 Sniffing

- A sniffer can be a packet capturing or frame capturing tool.
- Sniffer intercepts traffic on the network and displays it in either a command-line or GUI format to view for a hacker.
- Some sophisticated sniffers interpret packets and can reassemble packet stream into the original data, such as an e-mail or a document.
- It is used to capture traffic sent between two systems.
- Hacker can use a sniffer to discover usernames, passwords, and other confidential information transmitted on the network depending on how the sniffer is used and the security measures in place.
- There are several hacking attacks and various hacking tools require the use of a sniffer to obtain important information sent from target system.
- Sniffer software works by capturing packets not destined for the systems MAC address but rather for a targets destination MAC address. This is known as promiscuous mode.
- A system on the network reads and responds only to traffic sent directly to its MAC address.
- The system reads all traffic and sends it to the sniffer for processing in promiscuous mode.
- This mode is enabled on a network card with the installation of special driver software.
- Many of the hacking tools used for sniffing include a promiscuous-mode driver to facilitate this process.
- Any protocols that don't encrypt data are susceptible to sniffing. Protocols such as HTTP, Simple Network Management Protocol, POP3, and FTP are most commonly captured using a sniffer and viewed by hacker to gather valuable information such as usernames and passwords.
- There are two different types of sniffing:
  1. Passive sniffing
  2. Active sniffing.

1. Passive sniffing

- It involves listening and capturing traffic, and is useful in a network connected by hubs.
- Passive sniffing isn't detectable.

2. Active sniffing

- It involves launching an Address Resolution Protocol (ARP) spoofing or traffic-flooding attack against a switch in order to capture traffic.
- Active sniffing is detectable.
- All hosts on the network can see all traffic in networks that use hubs or wireless media to connect systems, therefore the passive packet sniffer can capture traffic going to and from all hosts connected via hub.
- A switched network operates differently. The switch looks at data sent to it and tries to forward packets to their intended recipients based on MAC address.
- The switch maintains the MAC table of all the systems and the port numbers to which they are connected.
- This enables the switch to segment the network traffic and send traffic only to correct destination MAC addresses.
- A switch network has greatly improved throughput and is more secure than the shared network connected via hubs.

Chapter Ends...

❑❑❑