VIT UNIVERSITY
SCHOOL OF COMPUTER SCIENCE ENGINEERING

UNIT 04

Vulnerability Analysis

Output of this Presentation

- Students will be able learn about the vulnerability and its types , this presentation also going to explain about the various model and tools of vulnerability analysis, this presentation brings learning for protecting our system from various attacks and vulnerable activities.

What is Vulnerability?

- Vulnerability can be defined as an issue in the software code that a hacker can exploit to harm the systems. It can be a gap in the implementation of cybersecurity procedures or a weakness in the controls.

What is an example of vulnerability?

- **Examples of vulnerabilities exist in every industry. These include:**
- Unauthorized network access by Hackers due to a weak Firewall
- Cracking of Wi-Fi Passwords
- Exposure of sensitive data due to lack of application security
  - Credit card data, Health Records
- Security misconfiguration
  - Misconfiguration of passwords
- Insecure cryptographic storage

Types of Vulnerability

The 4 main types of vulnerabilities are:

1. **Faulty defenses –** Poor defense measures pave the way for easy intrusion by hackers. This may be due to weak authentication, authorization, and encryption.
2. **Resource management not adequate –**The chances of buffer overflow and the potential to have many vulnerabilities are greater when there is inadequate resource management.

Types of Vulnerability

1. **Insecure connections –** If the connection between the system, application and networks is insecure, there is a higher probability of many threats like SQL injection.
2. **End user errors and misuse –** In many cases, the errors are caused by humans and misuse of the systems.

What are vulnerabilities?

1. **Allowing Domains or Accounts to Expire**
   - When domain names have expired, the hacker may buy them and set up a mail server. The hacker can find out the incoming mails and get to know the details.
2. **Buffer Overflow**
   - A process where there is more data added to the buffer and the excess data becomes corrupted and susceptible to vulnerabilities.
3. **Business logic vulnerability**
   - The software code may be missing a security control like authentications, encryption, or authorization.

-

What are vulnerabilities? Cont..

4. **CRLF Injection**

   Carriage Return Line Feed – Can be done by modifying the HTTP parameter of the URL.

5. **CSV Injection**

   When untrusted CSV files are embedded to the websites causing vulnerabilities.

6. **Catch Null Pointer Exception**

   When the program contains the null pointer, it is highly risky.

7. **Covert storage channel**

   This can help the attackers easily and often happens due to faulty implementation.

8. **Deserialization of untrusted data**

   Injection of malicious data into the applications to stop execution of programs.

What are vulnerabilities? Cont..

9. **Directory Restriction Error**

   Happens due to the improper use of CHROOT.

10. **Doubly freeing memory**

    This error occurs when free() is called more than once in the memory address.

11. **Empty String Password**

    Empty string password is highly insecure.

12. **Expression Language Injection**

    Injection happens when attacker-controlled data enters an EL interpreter.

13. **Full Trust CLR Verification issue Exploiting Passing Reference Types by Reference**

    Create a file called by ValueTypeTest.cs and compile it using csc by Value Type Test.csc.

What are vulnerabilities? Cont..

14. **Heartbleed Bug**

    Catastrophic bug in OpenSSL

15. **Improper Data Validation**

    Multiple validation forms with the same name indicate that validation logic is not up-to-date.

16. **Improper pointer subtraction**

    The subtraction of one pointer from another to determine the size is dependent on the assumption that both pointers exist in the same memory chunk.

17. **Information exposure through query strings in url**

    Information exposure through query strings in URL is when sensitive data is passed to parameters in the URL.

What are vulnerabilities? Cont..

18. **Injection problem**

    The basic form of this flaw involves the injection of control-plane data into the data-plane in order to alter the control flow of the process

19. **Insecure Compiler Optimization**

    Improperly scrubbing sensitive data from memory can compromise security.

20. **Insecure Randomness**

    Insecure randomness errors occur when a function that can produce predictable values is used as a source of randomness in security-sensitive context.

21. **Insecure Temporary File**

    Creating and using insecure temporary files can leave application and system data vulnerable to attacks.

22. **Insecure Third-Party Domain Access**

    Occurs when an application contains content provided from a 3rd party resource that is delivered without any type of content scrub.

What is Vulnerability Analysis?

- Vulnerability analysis is a procedure to check all the vulnerabilities in the systems, computers and other ecosystem tools. The vulnerability analysis helps in the analyzing, recognizing and ranking of the vulnerabilities as per the severity. It helps with the identification and assessment of threat details, enabling us to keep a resolution to protect them from hackers. The analysis can be done for every industry from Healthcare to Retail to IT.

Objectives of the Vulnerability analysis

1. To identify vulnerabilities – Configuration, system, Design, Code, Process
2. Documenting the vulnerabilities
3. Preparation of guidance to mitigate the vulnerabilities

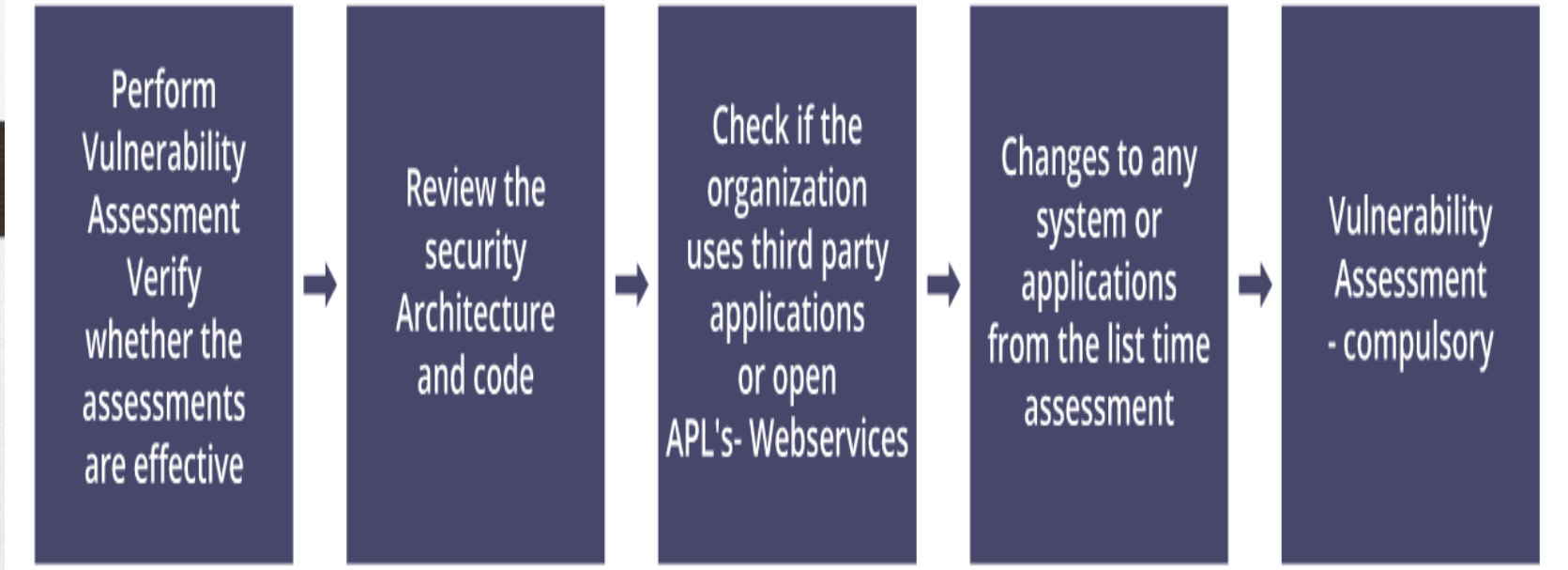
Importance of Vulnerability Analysis

- Deep dive insights of the security issues
- Helps us understand the risks associated with the entire ecosystem
  - For security breaches
- Assets that are prone to cyber attacks

Steps for the vulnerability Analysis

Step 1 Assess Critical Value of each device	Review all the devices in the network Who are the people accessing the devices Capture the below information Risk Impact Risk threshold Risk strategy planning Mitigation Business impact analysis
Step 2 Details of the installed systems	Systems – What they do For whom the devices are installed Review – Device open ports Configuration of the devices Drivers of the devices which are certified Device vendor, version details Software installed on the devices Software installed on the devices
Step 3 Vulnerability Scanning	Compliance requirements checking Scan Policy formation Scanning – Single or Multiple times
Step 4 Report Creation	Vulnerability name Vulnerability Discover date Common Vulnerabilities Risk Score, Systems affected Method to fix them

How to check if the organization requires Vulnerability Analysis



Types of Vulnerability Assessment Cont..

- **Network Based Scans**
- To identify network vulnerabilities. This scan helps to find the vulnerable systems in the wired and wireless networks

- **Host Based Scans**
- This scan is to identify vulnerabilities in the ports, configuration, server workstations, other hosts and patch history

Types of Vulnerability Assessment Cont..

- **Wireless Network Scans**

Complete scan on wireless networks to find the vulnerabilities

- **Application Scans**
- To test all portals and mobile applications for vulnerabilities
- **Database Scans**
- To scan all the databases for potential vulnerabilities

Models of Vulnerability in Ethical Hacking

- **Firewall model**
- Insider attacks - A Perimeter firewall should be decided and this can take care of the external attacks
- Missed security patches
  - When the patch management of firewall has not happened
- Configuration issues
  - If there are faults in the configuration of firewall
- DDOS attacks
  - Only allow legitimate traffic to avoid these attacks

Models of Vulnerability in Ethical Hacking cont..

- **Password model**
- To crack the password the hacker uses any of the following – Dictionary, Hybrid model and Brute force
- **Logical Bombing**
- This usually happens when the hacker uses a malicious code to inject the web application or the cloud infrastructure
- **Web Hijacking**
- This happens when an unauthorized user tries to access the application bypassing the authorization mechanism

Protection from Hacking

We need to follow some simple steps to prevent hacking

- Updating of Operating systems
- Installation of the proper firewall to prevent intrusion
- Destroying all personal information from all the web sources
- No use of Open Wi-Fi
- Password – Strong password which is not easy to find out
- Smart emailing – Avoid opening of phishing mails
- Keep the sensitive data in the protected environment
- Ignore spam
- Shut down the systems after use
- Secure the network
- Back up the data

Vulnerability Assessments

- There are type of vulnerability assessments below:
- **Active assessments –** Which is the process to send request to the live network directly.
- **Passive assessments** – Which is the process discover vulnerabilities, open ports, and etc without sending request the target hosts.
- **External assessments** – Here hackers use techniques to find vulnerabilities of system from outside.
- **Internal assessments –** Here hackers use techniques to find vulnerabilities of system from internally.

The Vulnerability assessments Life Cycle allow organizations to identify system security weaknesses, prioritize assets, and remediate that and verify that they have been eliminated. There are following phases of the Vulnerability assessments Life Cycle:

Vulnerability Assessments

- **Creating Baseline** – Here performing assessment to find out details including hosts, network, application and other open services.
- **Vulnerability Assessment** – Here collecting all found vulnerabilities of the system and priorities that .
- **Risk Assessment** – Here defining the impact of vulnerabilities to an organization
- **Remediation** – Here prioritize and fix vulnerabilities in order according to business risk
- **Verification** – Here verifying that all vulnerabilities have been eliminated on organizations.
- **Monitor** – The end always must monitoring the network and system to avoid unsuspected attacks.

Conclusion

- In this article we have discussed the various vulnerabilities that hackers can exploit to gain unauthorized access to a system. Best practices and techniques on how to find the vulnerabilities are also discussed. We have discussed the analysis of vulnerabilities and how it helps in preventing the system from being hacked. Finally, we have discussed models of vulnerabilities in ethical hacking and the ways to keep ourselves protected from hacking.

Question Please?