SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

VI SEMESTER

1923602 – VULNERABILITY DISCOVERY & EXPLOIT DEVELOPMENT

Regulation – 2019

Academic Year 2024-2025 (Even Semester)

Prepared by

Ms. C. Jesifica Cinthamani, A.P (O.G) / CYS

SUBJECT: 1923602 – VULNERABILITY DISCOVERY & EXPLOITDEVELOPMENT
SEM/YEAR: VI / III

UNIT I - INTRODUCTION TO VULNERABILITY DISCOVERY

Background: Vulnerability Discovery Methodologies – Fuzzing Methods and Fuzzer Types, Data Representation and Analysis – Requirements for Effective Fuzzing.

Vulnerability Issues: Operating System Vulnerabilities – Application Vulnerabilities – Connectivity and Dependence – Vulnerability assessment for natural disaster, technological hazards, and terrorist threats.

PART – A

Q.No	Question	Level	Competence
1	List some of the Vulnerability Discovery Methodologies.	BTL3	Applying
2	Point out the need for using Whitebox Testing..	BTL4	Analyzing
3	What is BlackBox testing?	BTL1	Remembering
4	Discuss about the tools used for Vulnerability Discovery.	BTL2	Understanding
5	Outline the advantages of Black Box testing.	BTL2	Understanding
6	Explain with an example about Manual testing.	BTL1	Remembering
7	Define Fuzzing.	BTL1	Remembering
8	Define Reverse Code Engineering.	BTL1	Remembering
9	Explain the Pros and Cons of Black box testing.	BTL2	Understanding
10	Define the limitations of Fuzzing.	BTL1	Remembering
11	Generalize your view about Memory Corruption.	BTL6	Creating
12	Infer the advantages and disadvantages of Manual testing.	BTL4	Analyzing
13	Identify what is multistage vulnerability?	BTL3	Applying
14	Define Pregenerated test cases.	BTL2	Understanding
15	Show the Fuzzing Methods.	BTL3	Applying
16	Assess the term Mutation testing.	BTL5	Evaluating
17	List the Phases of Fuzzing.	BTL1	Remembering
18	Point out the fuzzer types.	BTL4	Analyzing
19	Discuss Protocols.	BTL6	Creating
20	Assess the Protocol fields in detail.	BTL5	Evaluating
21	Identify why we need to use protocols.	BTL3	Applying
22	What are Remote fuzzers?	BTL2	Understanding
23	Differentiate between Black box and white box testing.	BTL4	Analyzing
24	Explain the benefits of using Protocols.	BTL5	Evaluating
25	Define Port Scanning	BTL2	Understanding

PART – B

Q.No	Question	Level	Competence
1	Explain Whitebox testing and the respective tools used in detail. (13)	BTL1	Remembering
2	With the help of a neat architecture diagram explain Blackbox and Manual testing. (13)	BTL1	Remembering
3	Describe in detail about application vulnerabilities with examples.(13)	BTL1	Remembering
4	(i) Describe about Binary Auditing.(7) (ii) Describe Automated Binary Auditing (6)	BTL2	Understanding
5	List the Phases of Fuzzing and explain the same in detail.(13)	BTL2	Understanding
6	(i)Describe in detail about Fuzzing Limitations and Expectations. (5) (ii) Explain the requirements of effective fuzzing. (8)	BTL1	Remembering
7	Examine about the Manual Protocol Mutation testing in detail. (13)	BTL3	Applying

8	Explain the following: i) Brute Force testing. (7) ii) Automatic Protocol generation testing. (6)	BTL4	Analyzing
9	Explain in detail about Local fuzzer and its types. (13)	BTL4	Analyzing
10	Explain the Remote Fuzzers and its types. (13)	BTL2	Understanding
11	Compare and contrast the Local and Remote fuzzers.	BTL3	Applying
12	Explain Web Application Fuzzers in detail (13)	BTL6	Creating
13	Explain Fuzzer Frameworks in detail. (13)	BTL 5	Evaluating
14	Analyze and Explain the protocol fields. (13)	BTL4	Analyzing
15	Briefly explain Network protocols. (13)	BTL2	Understanding
16	(i)Examine some operating system vulnerabilities with suitable examples.(8) (ii)Explain the measures for securing OS. (5)	BTL3	Applying
17	Define Vulnerability assessment for natural disaster and explain in detail.(13)	BTL 5	Evaluating

PART - C			
Q.No	**Question**	**Level**	**Competence**
1	Explain the Vulnerability Discovery Methodologies in detail. (15)	BTL5	Evaluating
2	Discuss the Fuzzing Methods and Fuzzer types in detail. (15)	BTL6	Creating
3	Discuss on Data Representation and Analysis strategies in Detail. (15)	BTL6	Creating
4	Explain the Operating system and Application Vulnerabilities in brief. (15)	BTL5	Evaluating
5	With the help of an example explain the technological and terrorist threats. (15)	BTL5	Evaluating

UNIT –II ADVANCED FUZZY TECHNOLOGIES

Targets and Automation: Automation and Data Generation – Environment Variable and Argument Fuzzing – Web Application and Server Fuzzing – File Format Fuzzing – Network Protocol Fuzzing – Web Browser Fuzzing – In–Memory Fuzzing.

Advanced Fuzzy Technologies – Fuzzing Frameworks – Automated Protocol Dissection – Fuzzer Tracking – Intelligent Fault Detection.

PART-A

Q.No	Question	Competence	Level
1	What is Fuzz Testing?	Remembering	BTL1
2	What is white box testing?	Remembering	BTL1
3	Define the term reverse engineering.	Remembering	BTL1
4	Explain web application fuzzing.	Evaluating	BTL5
5	Classify the different network protocol fuzzers.	Applying	BTL3
6	Write about the disadvantages of source code analysis.	Remembering	BTL1
7	Explain the term Event log.	Analysing	BTL4
8	Differentiate between disassembler and decompiler.	Understanding	BTL2
9	Summarize the classes of vulnerabilities that typically goes undiscovered by a fuzzer?	Understanding	BTL2
10	Differentiate White box and black box testing.	Understanding	BTL2
11	Does the fuzzer need to know how the protocol is used in a normal situation to understand an anomaly caused by security vulnerability?	Creating	BTL6
12	What are the techniques used for intelligent fault detection?	Remembering	BTL1
13	Discuss Microsoft fuzz?	Understanding	BTL2
14	What are the 5 fuzzing categories?	Remembering	BTL1
15	Discover vulnerable libraries.	Applying	BTL3
16	Examine Mucinac –ab.	Applying	BTL3
17	Analyse the tools and libraries that helps in the design and implementation phase of fuzzer.	Analysing	BTL4
18	Explain about reverse engineering.	Evaluating	BTL5
19	Classify the different fuzzy phases.	Analysing	BTL4
20	Prepare a note on remote code execution.	Creating	BTL6
21	List out the Pros and Cons of Fuzz Testing.	Understanding	BTL2
22	Explain DoS attack. Give example.	Evaluating	BTL5
23	Examine Backdoor.	Applying	BTL3
24	Explain Buffer Overflow attack.	Analysing	BTL4

PART-B

Q.No		Question	Marks	Competence	Level
1	**-**	Describe in detail about test data generation.	13	Remembering	BTL1
2	**A**	Summarize the phases of fuzzing.	07	Evaluating	BTL5
	B	Compare and contrast fuzzing and it's types.	06		
3	**-**	Discuss the types of bugs detected by Fuzz Testing.	13	Understanding	BTL2
4	**-**	Discuss the detection approach in file format fuzzing.	13	Understanding	BTL2
5	**-**	Illustrate the vulnerabilities in web application.	13	Applying	BTL3
6	**A**	Explain in detail about fuzzing.	07	Analysing	BTL4
	B	Explain the advantages and disadvantages of fuzzing.	06		
7	**A**	List out the web application vulnerability that can be identified by fuzzing.	07	Remembering	BTL1
	B	Name the file format fuzzing and vulnerabilities related to file format.	06		
8	**-**	Analyze web browser fuzzing with its detection.	13	Analysing	BTL4

9	**-**	Describe Architecting a fuzzer tracker and process involved in tracing	13	Remembering	BTL1
10	**A**	Classify the detection approach in web browser.	07	Remembering	BTL1
	B	List in detail about proxy fuzzing and improved proxy fuzzing.	06		
11	**-**	Summarize the detection approach in file format.	13	Understanding	BTL2
12	**-**	Illustrate the types of bugs detected by Fuzz Testing.	13	Applying	BTL3
13	**-**	Classify the pros and cons of Fuzzing.	13	Applying	BTL3
14	**-**	Formulate the Dfuz framework.	13	Creating	BTL6
15	**-**	Discuss about Intelligent Fault Detection with examples.	13	Understanding	BTL2
16	**-**	Classify the file format fuzzing and vulnerabilities related to file format.	13	Analysing	BTL4
17	**-**	Evaluate web browser fuzzing.	13	Evaluating	BTL5
PART-C					
1	Evaluate Real Time Fault Detection and Diagnosis using Intelligent Monitoring and Supervision Systems.		15	Evaluating	BTL5
2	Develop Intelligent Fault Detection and Classification Based on Hybrid Deep Learning Methods for Hardware-in-the-Loop Test of Automotive Software Systems.		15	Creating	BTL6
3	Evaluate Automated Network Protocol Fuzzing Framework.		15	Evaluating	BTL5
4	Generalize in detail about Dfuz framework.		15	Creating	BTL6
5	Compare and contrast the merits and demerits of fuzzing.		15	Creating	BTL6

UNIT–III LINUX EXPLOITATION

Advanced Linux Exploitation: Linux heap management, constructs, and environment, Navigating the heap – Abusing macros such as unlink() and frontlink() – Function pointer overwrites – Using IDA for Linux application exploitation – , – One day Exploits and Return Oriented Shellcode. Microsoft patch management process and Patch Tuesday – Obtaining patches and patch extraction – Binary diffing with BinDiff, patchdiff2, turbodiff, and darungrim – Triggering patched vulnerabilities – Writing one–day exploits – Handling modern exploit mitigation controls.

PART-A

Q.No	Question	Competence	Level
1	What is Linux Exploitation?	Remembering	BTL1
2	What are the different types of Exploitation Tools?	Remembering	BTL1
3	Explain how to manage heap	Evaluating	BTL5
4	Define Process virtual memory	Remembering	BTL1
5	How to Check Memory Usage in Linux?	Analysing	BTL4
6	What is mean by Unlink Exploit	Remembering	BTL1
7	Explain the function frontlink()	Applying	BTL3
8	Discuss about Function Pointers	Understanding	BTL2
9	Summarize about Pointer Subterfuge	Understanding	BTL2
10	What is mean by IDA?	Understanding	BTL2
11	Does the IDA pro is the best disassembler in business? Justify your answer	Creating	BTL6
12	What are the list of commonly used options in diff?	Remembering	BTL1
13	How to use diff and patch?	Applying	BTL3
14	What is mean by Exploits and Return Oriented Shellcode?	Remembering	BTL1
15	Discover Return Oriented Shellcode.	Applying	BTL3
16	Discuss Microsoft patch management process?	Understanding	BTL2
17	Analyse the tools and libraries that helps in the Linux heap management	Analysing	BTL4
18	Explain how to Obtaining patches and patch extraction.	Evaluating	BTL5
19	Analyze Binary diffing with BinDiff.	Analysing	BTL4
20	Develop the Triggering patched vulnerabilities.	Creating	BTL6
21	List out the Pros and Cons of patched vulnerabilities	Understanding	BTL2
22	Explain Handling modern exploit mitigation controls..	Evaluating	BTL5
23	Examine day exploits	Applying	BTL3
24	Explain Return Oriented Shellcode	Analysing	BTL4

PART-B

Q.No		Question	Marks	Competence	Level
1	-	Describe about Linux heap management.	13	Remembering	BTL1
2	A	Summarize about Navigating the heap.	07	Evaluating	BTL5
	B	Discuss constructs and environment heap management	06		
3	-	Discuss about Abusing macros such as unlink() and frontlink().	13	Understanding	BTL2
4	-	Discuss the Function pointer overwrites	13	Understanding	BTL2
5	-	Illustrate vulnerabilities in Triggering patched	13	Applying	BTL3
6	A	Explain in detail about IDA.	07	Analysing	BTL4
	B	Explain about One day Exploits	06		
7	A	Explain in detail about Return Oriented Shellcode	07	Remembering	BTL1
	B	Differentiate between One day Exploits and Return Oriented Shellcode	06		
8	-	Analyze Usage IDA for Linux application exploitation	13	Analysing	BTL4

9	**-**	Describe about Microsoft patch management process	13	Remembering	BTL1
10	**A**	Explain about Patch Tuesday –	07		
	B	Discuss in detail about Obtaining patches	06	Remembering	BTL1
11	**-**	Summarize about Obtaining patches and patch extraction process	13	Understanding	BTL2
12	**-**	Illustrate about Binary diffing with BinDiff.	13	Applying	BTL3
13	**-**	Classify the pros and cons of patchdiff2, turbodiff, and darungrim	13	Applying	BTL3
14	**-**	Encrypt Writing one–day exploits	13	Creating	BTL6
15	**-**	Summarize the how to Handle modern exploit mitigation controls.	13	Understanding	BTL2
16	**-**	Analyse turbodiff concept	13	Analysing	BTL4
17	**-**	Evaluate darungrim methodology	13	Evaluating	BTL5
PART-C					
1		Analyze Linux heap management and constructs the tools needed for Heap management	15	Creating	BTL6
2		Evaluate IDA for Linux application exploitation.	15	Evaluating	BTL5
3		Analyze the difference between Obtaining patches and patch extraction	15	Analysing	BTL4
4		Generalize in detail about Handling modern exploit mitigation controls	15	Creating	BTL6
5		Analyze about Microsoft patch management process	15	Analysing	BTL4

UNIT – IV : WINDOWS EXPLOITATION

Windows Kernel Debugging and Exploitation: Understanding the Windows Kernel, WinDbg, Analysing Kernel vulnerabilities and Kernel vulnerability types, Kernel exploitation techniques. **Windows Heap Overflows and Client–Side Exploitation:** Windows heap management, constructs, and environment – Browser–based and client–side exploitation, Remedial heap spraying, vftable/vtable behavior, Modern heap spraying to determine address predictability, Use–After–Free attacks and dangling pointers, Determining exploitability, Defeating ASLR, DEP, and other common exploit mitigation controls.

PART-A

Q.No	Question	Competence	Level
1	Differentiate between execution protection and access protection.	Applying	BTL3
2	Point out the importance of Windows Kernel.	Analyzing	BTL4
3	List any five components of Windows Kernel.	Remembering	BTL1
4	Discuss about Kernel Vulnerabilities.	Understanding	BTL2
5	Define WinDbg.	Understanding	BTL2
6	List the types of Kernel Vulnerabilities.	Remembering	BTL1
7	Define Windows heap management.	Remembering	BTL1
8	List the Kernel Exploitation Techniques.	Remembering	BTL1
9	Differentiate vftable and vtable.	Understanding	BTL2
10	Define ASLR.	Remembering	BTL1
11	Generalize your view about heap spraying attack.	Creating	BTL6
12	Analyze dangling pointers.	Analyzing	BTL4
13	Distinguish between Data execution prevention and Structuted exceptionhandling.	Applying	BTL3
14	Define DEP.	Understanding	BTL2
15	Show the advantages of WinDbg.	Applying	BTL3
16	Assess the various levels of vulnerabilities.	Evaluating	BTL5
17	List the memory management technique used in windows.	Remembering	BTL1
18	Compare: heap spraying and password spraying.	Analyzing	BTL4
19	Investigate client side exploitation.	Creating	BTL6
20	Assess the characteristics that distinguish the linux kernel with windowskernel.	Evaluating	BTL5
21	List the role of Linux kernel.	Applying	BTL3
22	What are mitigating controls?	Understanding	BTL2
23	Differentiate between ASLR and DEP.	Analyzing	BTL4
24	Explain the concept of windows heap overflow.	Evaluating	BTL5

PART-B

Q.No		Question	Marks	Competence	Level
1	-	Describe in detail about Windows Kernel	13	Remembering	BTL1
2	**A**	List the advantages of Linux Kernel.	07	Remembering	BTL1
	B	List the importance of WinDbg.	06		
3	-	Describe in detail about Browser Based Exploitation.	13	Remembering	BTL2
4	-	(i) Describe about kernel vulnerabilities. (6) (ii) What are the types of kernel vulnerabilities? (7)	13	Understanding	BTL2
5	-	Briefly explain about Windows heap management. (13)	13	Understanding	BTL2
6	**A**	Describe about the Kernel Exploitation techniques. (13)	07	Remembering	BTL1

7	**A**	Examine about vftable behaviour.	07	..	BTL3
	B	vtable behavior.	06	Applying	
8	**A**	Explain the following: ASLR	3	Analysing	BTL4
	B	DEP	3		
	C	Structured Exception handling	07		
9	**A**	Explain a note on dangling pointers.	06	Analysing	BTL4
	B	How do you handle dangling pointers	07		
10	**-**	Describe in detail about client side exploitation.	(13)	Analysing	BTL4
11	**A**	Compare the following Heap Spraying	07	Applying	BTL3
	B	Password Spraying	06		
12	**A**	Discuss about the functions of heap management? (8)	08	Creating	BTL6
	B	What is meant by the term use after free? (5)	05		
13	**-**	Explain in detail about common exploit mitigation controls . (13)	13	Evaluating	BTL5
14	**-**	Analyze and Explain about modern heap spraying to determine addresspredictability. (13)	13	Analysing	BTL4
15	**-**	Briefly explain about Remedial heap spraying. (13)	13	Understanding	BTL2
16	**-**	Compare Linux Kernel and Windows Kernel. (13)	13	Applying	BTL3
17	**-**	Explain in detail about the steps taken in defeating ASLR and DEP. (13)	13	Evaluating	TL5
PART-C					
1	Explain in detail about various Kernel Exploitatation Techniques? (15)		15	Evaluating	BTL5
2	Describe the basic architecture of a Windows Kernel with the help of the blockdiagram. (15)		15	Creating	BTL6
3	What is meant by WinDbg? How do you use WinDbg step by step? (15)		15	Creating	BTL6
4	Compare and contrast about Windows Kernel and Linux Kernel. (15)		15	Evaluating	BTL5
5	Explain in detail about the Windows Heap Overflows. (15)		15	Evaluating	BTL5

UNIT – V : ANDROID AND iOS EXPLOITATION
Android Exploitation: Android Basics, Android Security Model, Introduction to ARM, Android Development Tools, Android Security Assessment Tools, Exploiting Applications, Protecting Applications, Native Exploitation and Analysis. **iOS Exploitation**: Introduction to iOS hacking, iOS User Space Exploitation, iOS Kernel Debugging and Exploitation.

PART – A

Q.No	Question	Level	Competence
1	Differentiate between Android and ios	BTL3	Applying
2	Point out the importance of Android	BTL4	Analyzing
3	List the categories of Android applications.	BTL1	Remembering
4	Discuss about ARM.	BTL2	Understanding
5	Define android and ios.	BTL2	Understanding
6	List the android development tools	BTL1	Remembering
7	Define Android Security Model.	BTL1	Remembering
8	List the Android security assessment tools.	BTL1	Remembering
9	Discuss the features of Android.	BTL2	Understanding
10	Define ios attacks .	BTL1	Remembering
11	Generalize the steps to protect your android application	BTL6	Creating
12	Analyze content provider in android.	BTL4	Analyzing
13	List the phases of hacking.	BTL3	Applying
14	Define ios kernel debugging.	BTL2	Understanding
15	Show the advantages of Android applications.	BTL3	Applying
16	Assess the features of ARM processor	BTL5	Evaluating
17	List the components of Android	BTL1	Remembering
18	Compare: Native Exploitation and Indigenous Exploitation.	BTL4	Analyzing
19	Investigate how do you protect your android from harmful applications.	BTL6	Creating
20	Assess the characteristics of Android Debug Bridge..	BTL5	Evaluating
21	List the ios hacking applications.	BTL3	Applying
22	What is kernel mode debugging?	BTL2	Understanding
23	Differentiate between content provider and content resolver in android.	BTL4	Analyzing
24	Judge whether hacking possible in ios.	BTL5	Evaluating

PART – B

Q.No	Question	Level	Competence
1	Describe various features of android applications. (13)	BTL1	Remembering
2	(i) List the disadvantages of android applications. (6) (ii) List the various components of Android .(7)	BTL1	Remembering
3	Describe in detail about Android Security model.(13)	BTL1	Remembering
4	(ii) Describe about user data of Android. (5) (ii) List the permissions check required for accessing the sensitive user data(8)	BTL2	Understanding
5	Construct the architecture of Android software stack. (13)	BTL2	Understanding
6	Describe about ARM processor. (13)	BTL1	Remembering

7	Examine about (i) Android Development tools. (6)	BTL3	Applying
	(ii)Android Security tools..(7)		
8	Explain the following: iii) Protecting Android applications. (7) iv) Exploiting Android applications. (6)	BTL4	Analyzing
9	(i) Explain about the components of Android. (6) ii)Analyze how the data storage occur in android applications (7)	BTL4	Analyzing
10	Draw the architecture diagram for android security model.(13)	BTL2	Understanding
11	Compare the following (i) ios (6) (ii) Android (7)	BTL3	Applying
12	i) Discuss the main characteristics of ios (6) ii) Explain about ios hacking applications (7)	BTL6	Creating
13	Demonstrate the security features to build the security android applications. (13)	BTL 5	Evaluating
14	Analyze ios hacking with an example. (13)	BTL4	Analyzing
15	Briefly explain the steps involved in ios kernel debugging. (13)	BTL2	Understanding
16	Examine the phases of ios hacking. (13)	BTL3	Applying
17	Explain the following. i) iOS User Space Exploitation (6) ii) iOS Kernel Debugging and Exploitation. (7)	BTL 5	Evaluating

PART - C			
Q.No	**Question**	**Level**	**Competence**
1	Explain the following i) Kernel debugging with an example (5) ii) How do I debug an ios device? (5) iii) Compare user mode debugging and kernel mode debugging. (5)	BTL5	Evaluating
2	i) Explain the steps for developing various ios hacking tools. (8) ii) Explain the steps for developing android security assessment tools. (7)	BTL6	Creating
3	Develop an android application on your own and discuss about the steps in developing an android application(15)	BTL6	Creating
4	Compare the features of various Android development tools. (15)	BTL5	Evaluating
5	With the help of a neat block diagram explain the basic architecture of android application.(15)	BTL5	Evaluating