COMPUTER CRIME AND SECURITY (CE436)

VA SCAN

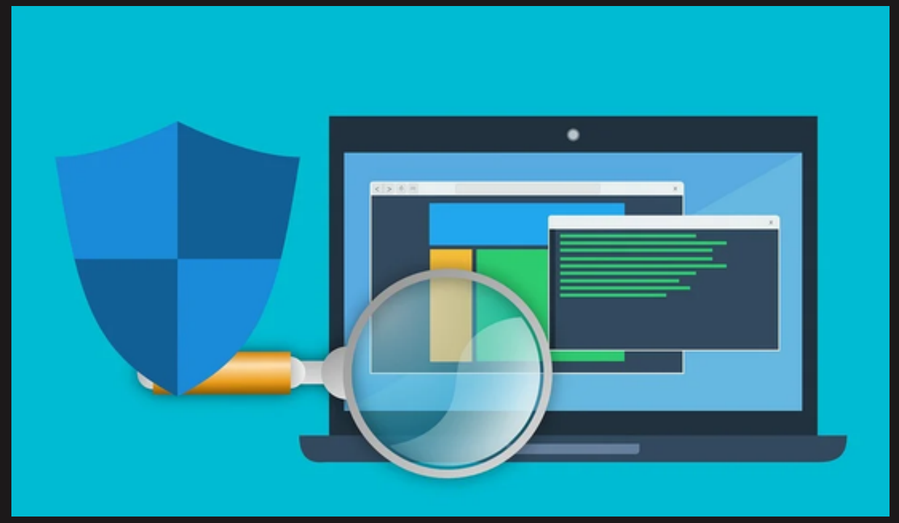
VULNERABILITY SCANNING

รายชื่อสมาชิกกลุ่ม

นายภูริพัฒน์	รัตนยืนยง	1620900579
นางสาวกานต์กนก	เลิศไธสงค์	1620900884
นายกิติคุณ	สุวรรณคีรี	1620902062

WHAT IS VA SCAN?

Vulnerability Assessment เป็นการตรวจสอบอย่างเป็นระบบในเรื่องของการหาช่องโหว่ทางด้านความความปลอดภัย โดยจะใช้การประเมินว่าระบบนั้นจะสามารถโดนเจาะได้ผ่านทางไหนได้บ้าง ด้วยการโจมตีลักษณะใดได้บ้าง และก็จะแนะนำให้อุดช่องโหว่เหล่านั้น



VA Scan จะดำเนินการโดยใช้เครื่องมืออัตโนมัติที่จะสแกนระบบเป็นระยะเพื่อหาจุดอ่อนที่อาจเกิดขึ้น

THREAT

ตัวอย่างภัยคุกคามที่สามารถหลีกเลี่ยงไม่ให้เกิดขึ้นได้ด้วยการทำ VA Scan

1

SQL injection, XSS และ
การโจมตีแบบ Code
Injection แบบอื่น ๆ

2

การปลอมแปลงสิทธิ์ในการ
เข้าถึงระบบให้สูงขึ้น

3

ใช้ Software ในการแก้ไข
Setting ต่าง ๆ ให้ความ
ปลอดภัยลดลง

TYPES OF VA SCAN

รูปแบบของการทำ VA Scan มี 4 ส่วน ดังนี้

HOST SCANS

การประเมินความเสี่ยงในส่วนของ Server ที่มีความสำคัญ ซึ่งอาจจะเป็นเป้าหมายในการโจมตีได้หากไม่ได้รับการทดสอบอย่างเพียงพอ

DATABASE SCANS

การประเมินความเสี่ยงในเรื่องของ Database หรือระบบที่เกี่ยวข้องกับข้อมูล เช่น Big Data จะใช้การตรวจสอบจาก Database ที่ความปลอดภัยหละหลวม หลังจากนั้นจะทำการจัดลำดับความสำคัญของข้อมูล

NETWORK & WIRELESS SCANS

การประเมินความเสี่ยงโดยมีการกำหนด Policy และนำไปปฏิบัติจริงเพื่อป้องกันไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต

APPLICATION SCANS

ใช้วิธีการระบุช่องโหว่ทางด้านความปลอดภัยใน Web Application และ Source Code โดยการ Scan แบบอัตโนมัติที่ Front-end หรือไม่ก็วิเคราะห์ที่ Source Code

ขั้นตอนการทำ VA SCAN

1. ทดสอบ (Testing)
2. วิเคราะห์ (Analysis)
3. ประเมิน (Assessment)
4. แก้ไข (Remediation)

01 ทดสอบ (TESTING)

การระบุช่องโหว่ โดยใช้วิธีทดสอบจุดประสงค์ของขั้นตอนนี้คือการเตรียมรายการของช่องโหว่ใน Application ผู้ที่วิเคราะห์จะทำการทดสอบความแข็งแรงของระบบ Security ของ Application, Server หรือระบบอื่น ๆ โดยใช้เครื่องมือในการ Scan ระบบให้โดยอัตโนมัติ

02 วิเคราะห์ (ANALYSIS)

การวิเคราะห์ช่องโหว่และภัยคุกคามจุดประสงค์ของขั้นตอนนี้คือการหาสาเหตุหรือต้นตอที่เจอช่องโหว่มาจากข้อที่ 1 ซึ่งขั้นตอนนี้รวมไปถึงการระบุรายละเอียดของการทำงานของระบบว่ามีการตอบสนองต่อช่องโหว่อย่างไร และสาเหตุของการเกิดช่องโหว่

03 ประเมิน (ASSESSMENT)

การประเมินความเสี่ยงจุดประสงค์ของขั้นตอนนี้คือการจัดลำดับความสำคัญของช่องโหว่ โดยจะทำการระบุเป็น Rank หรือ Score ว่าช่องโหว่ไหนร้ายแรงกว่ากัน โดยอ้างอิงมาจากปัจจัยเหล่านี้ระบบที่ได้รับผลกระทบข้อมูลอะไรบ้างที่เป็นความเสี่ยงง่ายต่อการโจมตีความรุนแรงของการโจมตีความเสียหายที่อาจเกิดขึนจากช่องโหว่

04 แก้ไข (REMEDIATION)

การแก้ไขคือ การอุดช่องโหว่ โดยส่วนใหญ่จะเป็นการร่วมมือกันระหว่างทีมงานที่ดูแลเรื่อง Security กับทีม Operation ซึ่งเป็นผู้ที่สามารถบอกได้ว่าการอุดช่องโหว่แบบใด ระดับไหนจะมีประสิทธิภาพสูงสุดโดยที่ไม่กระทบกับระบบปัจจุบัน หรืออาจจะกระทบน้อยลง