กรอบแนวทางในการดำเนินการ จัดทำ Penetration Testing เบื้องต้นสำหรับผู้ดูแลระบบ

Penetration Test เป็นกระบวนการทดสอบและจำลองเหตุการณ์ hack ระบบสารสนเทศ โดยใช้กลยุทธ์และ เครื่องมือที่เหมาะสมเพื่อเจาะเข้าสู่ระบบ ซึ่งจะช่วยให้ทราบจุดแข็งและจุดอ่อนของระบบ ทั้งนี้ระบบ สารสนเทศ จะต้องมีการบริหารจัดการด้านความปลอดภัยของข้อมูล เพื่อทำให้เกิดความปลอดภัยของข้อมูล ได้แก่

1. การจัดการด้านความปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่ายและระบบสารสนเทศ

- (1) การออกแบบระบบให้มีความปลอดภัย
- (2) การ update patch ระบบปฏิบัติการ
- (3) การติดตั้ง Software Antivirus
- (4) การตั้งค่า firewall บนเครื่องแม่ข่าย
- (5) การเข้ารหัสข้อมูลด้วยวิธีการต่าง ๆ เช่น วิธีรการ hash ข้อมูล, การใช้ช่องทาง ssl
- (6) การจัดการด้านสิทธิ์ของผู้ใช้งานระบบ
- (7) การ backup สำรองขอมูล
- 2. การป้องกันความปลอดภัยด้านระบบเครือข่าย
 - (1) การใช้งานอุปกรณ์ป้องกันความปลอดภัยของระบบเครือข่าย (firewall) , IDS/IPS

การตรวจจับผู้บุกรุก

- (2) การควบคุม Network Zone ต่างๆ
- (3) การจัดการด้านสถาปัตยกรรมเครือข่าย
- (4) การจัดการการเข้าถึงระบบเครือข่าย ระบบคอมพิวเตอร์ต่างๆ
- (5) การใช้งานโพรโทคอลต่างๆ
- (6) การจัดการความปลอดภัยทางด้าน physical control

ขั้นตอนจัดทำ Penetration Test ประกอบด้วย 5 ขั้นตอน ดังนี้

1. การวางแผนและการสำรวจ

เป็นขั้นตอนแรกเกี่ยวข้องกับการวางแผนเพื่อจัดเตรียมการโจมตี โดยเป็นการสำรวจรวบรวมข้อมูลใน ระบบให้ได้มากที่สุด อาจเป็นขั้นตอนที่ใช้เวลานานที่สุด ซึ่งมีกระบวนการตรวจสอบระบบ สังเกตช่องโหว่ และ วิธีที่องค์กรตอบสนองต่อการละเมิดระบบ โดยข้อมูลที่ค้นหามีตั้งแต่ชื่อและที่อยู่อีเมลของพนักงานของบริษัท ไปจนถึง topology ของระบบเครือข่าย ที่อยู่ IP และอื่นๆ สังเกตได้ว่าประเภทของข้อมูลหรือระดับความลึก ของการตรวจสอบจะขึ้นอยู่กับวัตถุประสงค์ที่กำหนดไว้สำหรับการตรวจสอบ วิธีการรวบรวมข้อมูลเช่น social engineering, dumpster diving, network scanning, domain registration information เป็นต้น

2. การสแกนระบบ

จากขั้นตอนการวางแผนและสำรวจ ผู้ทดสอบการเจาะระบบจะใช้เครื่องมือสแกนเพื่อสำรวจจุดอ่อน ของระบบและเครือข่าย โดยการสแกนระบบนี้ จะพบจุดอ่อนของระบบ ที่อาจใช้สำหรับการโจมตีได้ ตัวอย่างเช่น ระบบสารสนเทศ : Web Application มาตราฐานความปลอดภัย : OWASP (จัดทำขึ้นโดยองค์กรไม่แสวงหาผลกำไร) เครื่องมือ : WEBGOAT, DVWA, SQLi-Labs เพื่อสแกนหาจุดอ่อนของระบบ

3. การเข้าถึงระบบ

เมื่อเข้าใจถึงช่องโหว่ของระบบแล้ว ผู้ทดสอบการเจาะระบบจะพยายามเจาะเข้าระบบโดยใช้ ประโยชน์จากจุดอ่อนด้านความปลอดภัย ซึ่งผู้ทดสอบการเจาะระบบจะพยายามเปลี่ยนแปลงสิทธิ์บนระบบ เพื่อแสดงให้เห็นว่าผู้ทดสอบการเจาะระบบจะสามารถเข้าไปในสภาพแวดล้อมเชิงลึกของระบบได้อย่างไร

4. การเข้าถึงแบบถาวร

ขั้นตอนนี้เป็นการใช้ประโยชน์จากซ่องโหว่จากสิทธิ์การเข้าถึง เมื่อผู้ทดสอบการเจาะระบบตั้งหลักใน ระบบแล้ว ผู้ทดสอบการเจาะระบบจะรักษาการเข้าถึงและควบคุมการโจมตีที่จำลองไว้นานพอที่จะบรรลุผล สำเร็จและทำซ้ำเป้าหมายของแฮ็กเกอร์ที่เป็นอันตราย ดังนั้นในระยะนี้ผู้ทดสอบการเจาะระบบจึงพยายามรับ ระดับสิทธิ์สูงสุดในระบบ

5. การวิเคราะห์/รายงานขั้นสุดท้าย

เป็นการรายงานผลมาจากการทดสอบการเจาะ ในขั้นตอนสุดท้าย ทีมรักษาความปลอดภัยจะเตรียม รายงานโดยละเอียดซึ่งอธิบายขั้นตอนการทดสอบการเจาะระบบทั้งหมด ข้อมูลหรือรายละเอียดบางอย่างที่ ควรปรากฏ ได้แก่

- (1) ความร้ายแรงของความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบ
- (2) เครื่องมือที่สามารถเจาะระบบได้สำเร็จ
- (3) เน้นย้ำจุดที่มีการรักษาความปลอดภัยอย่างถูกต้อง
- (4) ช่องโหว่เหล่านั้นที่ต้องแก้ไขและวิธีป้องกันการโจมตีในอนาคต (คำแนะนำการแก้ไข)

ขั้นตอนนี้อาจมีความสำคัญที่สุดสำหรับทั้งสองฝ่าย เนื่องจากเจ้าหน้าที่ไอทีและผู้จัดการที่ไม่ใช่ฝ่าย เทคนิคมักอ่านรายงานนี้ จึงแนะนำให้แยกรายงานออกเป็นส่วนคำอธิบายทั่วไปและด้านเทคนิคเพิ่มเติม เช่น รายงานผู้บริหารและรายงานทางเทคนิค

• แนะนำเครื่องมือในการสแกนระบบแบบออนไลน์

เว็บไซต์ OpenVas Online Scan (<u>https://hostedscan.com/openvas-vulnerability-scan</u>) ข้อดี จะมีวิธีการประมวลผลหลายวิธี จากการ submit url เพียงครั้งเดียว ข้อเสีย เป็นการบอกจุดอ่อนคร่าวๆ ไม่ได้ลงลึกถึง detail มากนัก

นอกจากนี้ยังมีเว็บไซต์อื่นๆ เช่น <u>https://sitecheck.sucuri.net/</u> และ <u>https://pentest-</u> tools.com/website-vulnerability-scanning/website-scanner

- วิธีการใช้งาน (OpenVas Online Scan)
- 1. กรอก url ระบบสารสนเทศ หรือ หมายเลข ip address ที่ต้องการแสกนลงในเว็บไซต์

	Scan Report
OpenVAS Online Scan Online network vulnerability scanner for >50,000 security vulnerabilities	March 31, 2020 Summary This document reports on the results of an automatic security scan. All dates are dis- played using the timenone "Coordinated Universal Time", which is abbreviated "UTC". The task was "65:8515960c53005646542-586345360550056106411". The scan started as The Mar 31 20:13:18 2020 UTC and ended at The Mar 31 20:22:01 2020 UTC. The report first summarises the results found. Then, for each hous, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.
Try for free	Contents 1 Result Overview 2
beta.sut.ac.th	2 Results per Host 2 2.1 43.35.66.40 2 2.1.1 Low general/rep 2 2.1.2 Log general/rep 2 2.1.3 Log general/rep 3 2.1.4 Log general/rep 4 2.1.4 Log general/rep 13 2.1.5 Log general/rep 16

2. กรอก email address เพื่อรับผลการสแกน และกด submit เพื่อรับผลการตรวจสอบเว็บไซต์

	Scan Report
OpenVAS Online Scan	March 31, 2020
Online network vulnerability scanner for >50,000 security vulnerabilities	Summary This document reports on the results of an automatic security scan. All dates are dis- played using the timescase "Coordinated Universal Time", which is abbreviated "UTC". The task was "iss8317960c-53005a0fd642-6e3345300ec53005a0fd6411". The scan started at Tue Mar 31 201318 2020 UTC and ended at Tue Mar 31 30:22021 0202 UTC. The summarises the results found. Then, for each host, the report describes every issue found. Plasae consider the advice given in each description, in order to rectify the issue.
Try for free	Contents
beta.sut.ac.th	1 Result Overview 2 2 Results per Host 2
noc@sut.ac.th	2.1 45.33.56:40 2 2.1.1 Low general/tep 2 2.1.2 Log general/CPE-T 3 2.1.3 Log 443/rep 4 2.1.4 Log general/tep 13 2.1.5 Log general/tep 16

การวิเคราะห์ผล

1.ภายหลังการ sumbit url หรือ ip เข้าระบบสแกนออนไลน์ ระบบจะทำการแจ้งผลโดยส่งข้อมูลเข้า email ที่เราได้ให้ไว้ ซึ่งสามารถดูรายละเอียดการสแกนได้ดังตัวอย่างต่อไปนี้

กล่องจดหมายเข้า กระ	อง 🗸	Your HostedScan sign-in link is here!
HostedScan.com Scan report -] 4 new risks detected by OpenVAS on emeetin OpenVAS Report by HostedScan Security This email contains a summary o	0 14:48	no-reply=hostedscan.com@mg.hostedscan.com ในนามของ HostedScan.com <no-reply@hostedscan.com> วนนี้,13:33 Network Operation Center %</no-reply@hostedscan.com>
HostedScan.com	D	
Scan report - 2 new risks detected by Nmap on emeeting.su Nmap Report by HostedScan Security This email contains a summary of yo	13:37	เพื่อปกป้องความเป็นส่วนด้วของคุณ ได้มีการบล็อกเนื้อหาบางส่วนในข้อความนี้ ถ้าต่องการเบ็ดการใช้งานฟิเจอร์ที่บล็อกอีกครั้ง คลิกที่น ั
HostedScan.com	D	เพื่อแสดงเนื้อหาจากผู้ส่งนี้เสมอ คลิกที่นี่
Scan report - I 4 new risks detected by OWASP ZAP on emee OWASP ZAP Report by HostedScan Security This email contains a summar	13:34	Coons in museused
HostedScan.com Your HostedScan sign-in link is here! Scans in progress! Click the link below to see scan results, track scan progr	13:33	Click the link below to see scan results, track scan progress, and schedule more scans.
Administrator report Monthly-2022-03-26-1200 Please see attachment for report Monthly-2022-03-26-1200.	0 12:00	See Results

รูปภาพแสดงการแจ้งผลมาที่ email

2. เมื่อได้รับ email คลิ้กที่ see results เพื่อทราบผลการสแกน

	HostedScan Security		Dashboard Targets	Scans Risks Reports API Docs Pricing 🔘 🕶	
	Add Targets			New Scan	
Mo	ist Recent Risks				
	TITLE	SCAN TYPE	TARGET	THREAT	QOD ⑦ STATUS LAST ▼
>	nginx 0.6.18 - 1.20,0 1-byte Memory Overwrite Vulnerability	OPENVAS	emeeting.sut.ac.th	HIGH	30% OPEN 35 minutes ago
>	nginx <= 1:21:1 information Disclosure Vulnerability	OPENVAS	emeeting.sut.ac.th	нісн	30% OPEN 35 minutes ago
>	nginx 0.7.12 < 1.17.7 HTTP Request Smuggling Vulnerability	OPENVAS	emeeting.sut.ac.th	MEDIUM	30% OPEN 35 minutes ago
>	TCP timestamps	OPENVAS	emeeting.sut.ac.th	LOW	80% OPEN 35 minutes ago
>	Open TCP Port: 8008	NMAP	emeeting.sut.ac.th	MEDIUM	OPEN 1 hour ago
			S <mark>ee all 10 risks 🛃</mark>		
Мо	ist Recent Scans				
	TARGET(S) SCAN TYPE	STATE	PROGRESS	RESULTS	CREATED
>	emeeting.sut.ac.th OPENVAS	SUCCEEDED	100	POF XML	1 hour ago
>	emeeting.sut.ac.th OWASP_ZAP	SUCCEEDED	100	HTML JSON PDF XML	1 hour ago
>	emeeting.sut.ac.th NMAP	SUCCEEDED	100	HTML JSON PDF XML	1 hour ago
			See all 3 scans 🛃		

 ที่หัวข้อ Most Recent Risks ระบบแจ้งจุดอ่อนของระบบสารสนเทศ (อาจเลือกให้แสดงผลแบบ 10 อันดับเพื่อทราบจุดอ่อนอื่น ๆ โดยสามารถคลิกเลือกได้จากเมนู "See all 10 risks")

Ris	ks			
	TITLE	SCAN TYPE	TARGET	THREAT LEVEL
>	nginx 0.6.18 - 1.20.0 1-byte Memory Overwrite Vulnerability	OPENVAS	emeeting.sut.ac.th	HIGH
>	nginx <= 1.21.1 Information Disclosure Vulnerability	OPENVAS	emeeting.sut.ac.th	HIGH
>	nginx 0.7.12 < 4.17.7 HTTP Request Smuggling Vulnerability	OPENVAS	emeeting.sut.ac.th	MEDIUM
>	TCP timestamps	OPENVAS	emeeting.sut.ac.th	LOW
>	Open TCP Port: 8008	NMAP	emeeting.sut.ac.th	MEDIUM
>	Open TCP Port: 80	NMAP	emeeting.sut.ac.th	MEDIUM
>	Application Error Disclosure	OWASP_ZAP	emeeting.sut.ac.th	MEDIUM
>	X-Frame-Options Header Not Set	OWASP_ZAP	emeeting.sut.ac.th	MEDIUM
>	Information Disclosure - Debug Error Messages	OWASP_ZAP	emeeting.sut.ac.th	LOW
>	X-Content-Type-Options Header Missing	OWASP_ZAP	emeeting.sut.ac.th	LOW

• ตัวอย่างการแปลผล

- nginx ซึ่งเป็น web server ของระบบ outdate อาจทำให้เกิด memory overwrite ซึ่ง
 เป็น threat ระดับ High ควรแก้ไขโดยด่วน
- มีการเปิด port 8008 ซึ่งเป็น threat ระดับ medium ผู้ดูแลระบบสารสนเทศอาจ ดำเนินการปิด port ของเครื่องแม่ข่ายได้ หากไม่ได้มีการใช้งานผ่าน port ดังกล่าว เป็นต้น
- ไม่มีการ set ค่า x-frame-option header ซึ่งการตั้งค่าดังกล่าว จะสามารถป้องการวิธีการ 'ClickJacking' attacks. ได้

~

ทั้งสามารถ	เลือกเมนู	เพื่อสามารถทราบร	รายละเอียดเ	พิ่มเติมได้
X-Frame-Optic	ons Header Not Set		OWASP_ZAP	emeeting.sut.ac.th
Name	X-Frame-Optio	ons Header Not Set		
Description	X-Frame-Opti	ons header is not included in the HTTP re	esponse to protect	against <mark>'ClickJacking' attacks.</mark>
Solution	Most modern then you'll wa	Web browsers support the X-Frame-Opt int to use SAMEORIGIN, otherwise if you	ions HTTP header. never expect the p	Ensure it's set on all web pages returned age to be framed, you should use DENY. A
Reference	https://develo	pper.mozilla.org/en-US/docs/Web/HTTP/h	leaders/X-Frame-C	ptions
CWE Id	1021			
WASC Id	15			
Other Information				
	uri	http://emeeting.sut.ac.th		
	method	GET		
Instances	param	X-Frame-Options		
	attack			
	evidence			

4. ที่หัวข้อ Most Recent Risks ระบบได้ทำการสแกนระบบสารสนเทศ โดยวิธีการอื่น ๆ และสามารถ ออก report ตามแต่ละประเภทเครื่องมือ เพื่อทราบรายละเอียดหรือวิธีการแก้ไขจุดอ่อนของระบบ เพิ่มเติม ได้แก่

- รูปแบบการสแกนแบบ Openvas
- รูปแบบการสแกนแบบ OWASP ZAP
- รูปแบบการสแกนแบบ NMAP

สามารถเลือกดูรายงานได้ตามแต่ละหัวข้อ ที่เมนู "result"

Мо	st Recent Scans				
	TARGET(S)	SCAN TYPE	STATE	PROGRESS	RESULTS
>	emeeting.sut.ac.th	OPENVAS	SUCCEEDED	100	PDF XML
>	emeeting.sut.ac.th	OWASP_ZAP	SUCCEEDED	100	HTML JSON PDF XML
>	emeeting.sut.ac.th	NMAP	SUCCEEDED	100	HTML JSON PDF XML
			See all 3 so	tans 🛃	

ตัวอย่างการออก report Scan Report March 26, 2022 Summary This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "623eb39b5eb6840040dfbf15-623eb39d5eb6840040dfbf1d". The scan started at Sat Mar 26 06:33:41 2022 UTC and ended at Sat Mar 26 07:47:35 2022 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue. 2.1.1 High 80/tcp แจ้งจุดอ่อนที่พบ High (CVSS: 9.4) NVT: nginx 0.6.18 - 1.20.0 1-byte Memory Overwrite Vulnerability Product detection result cpe:/a:f5:nginx:1.16.1 Detected by nginx Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.113787) Summary

... continues on next page ...

2	RESULTS	PER	HOST

Vulnerability Detection Result	y.
Installed version: 1,16,1	แจงจุดออนทพบ
Fixed version: 1.20.1/1.21.0	
Installation	
path / port: 80/tcp	
Solution:	แจ้ง solution การแก้ไขปัญหา
Solution type: VendorFix	`
Update to version 1.20.1, 1.21.0 or later.	
Affected Software/OS	
Affected Software/OS	
ffected Software/OS ginx version 0.6.18 through 1.20.0. ote: The issue only affects aginy if the 'resolver' dire	ctive is used in the configuration

3

Vulnerability Insight

server.

A security issue in nginx resolver was identified, which might allow an attacker to cause 1-byte memory overwrite by using a specially crafted DNS response, resulting in worker process crash or, potentially, in arbitrary code execution.

• ข้อแนะนำ

นอกจากการดำเนินการแก้ไขจุดอ่อนของระบบสารสนเทศ ตามที่ได้รับทราบแล้ว ระบบสารสนเทศที่มี การให้บริการในรูปแบบเว็บไซต์ ควรจัดให้มีการใช้งานผ่านช่องทาง SSL ช่วยเพิ่มความปลอดภัยในการ สื่อสารข้อมูลบนเครือข่ายอินเตอร์เน็ต เนื่องจาก SSL ทำการเข้ารหัสข้อมูลระหว่างผู้ใช้กับเซิร์ฟเวอร์ ช่วยป้องกันการถูกดักจับหรือเปิดอ่านข้อมูลระหว่างทาง (sniffing) ได้ทั้งนี้ ท่านสามารถขอใช้งาน SSL certificate ได้ฟรี จากบริการของศูนย์คอมพิวเตอร์ สามารถดูรายละเอียดเพิ่มเติมได้ที่ <u>http://its.sut.ac.th/index.php?option=com_content&view=article&id=55</u>