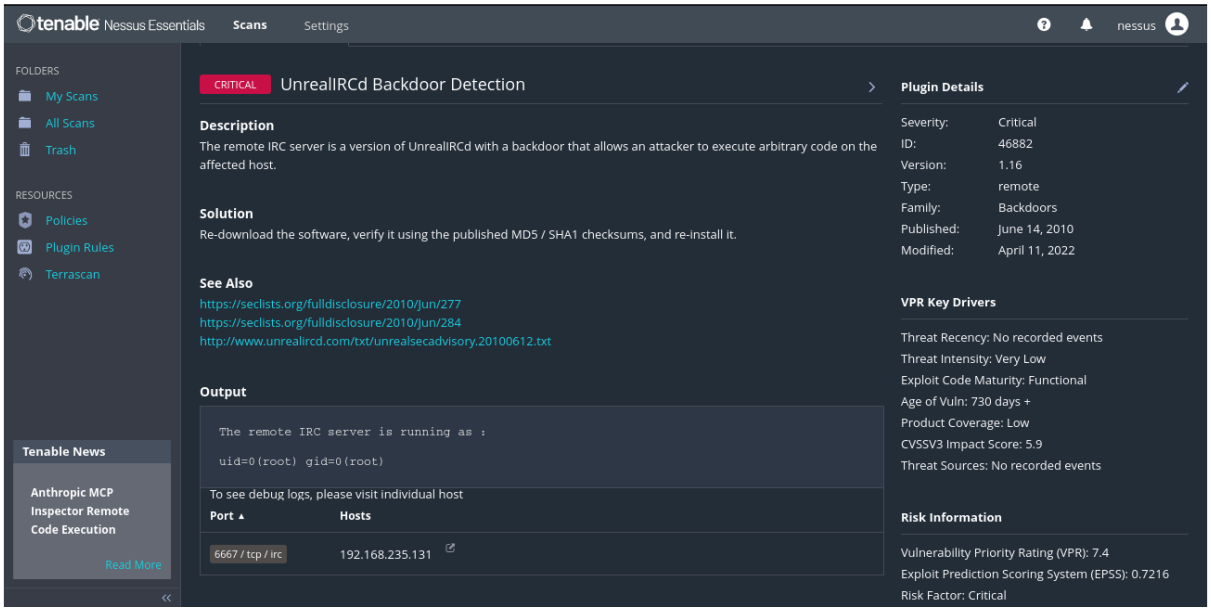
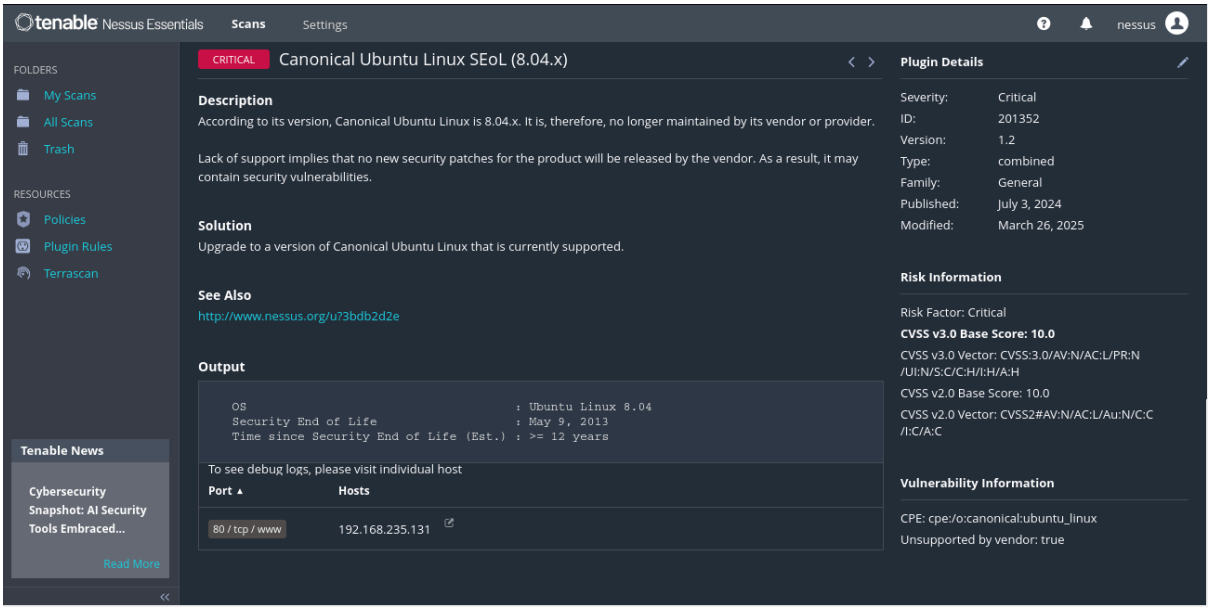
6604062636739 นายอดิกานต์ ทนุพันธ์

1. ให้ นักศึกษาส่งรายงาน การตรวจสอบ metasploit2 ที่ติดตั้งในเครื่องของตัวเอง มีช่องโหว่ระดับ CRITICAL ที่ port ใดบ้าง และรัน service อะไร โดยใช้ Nessus

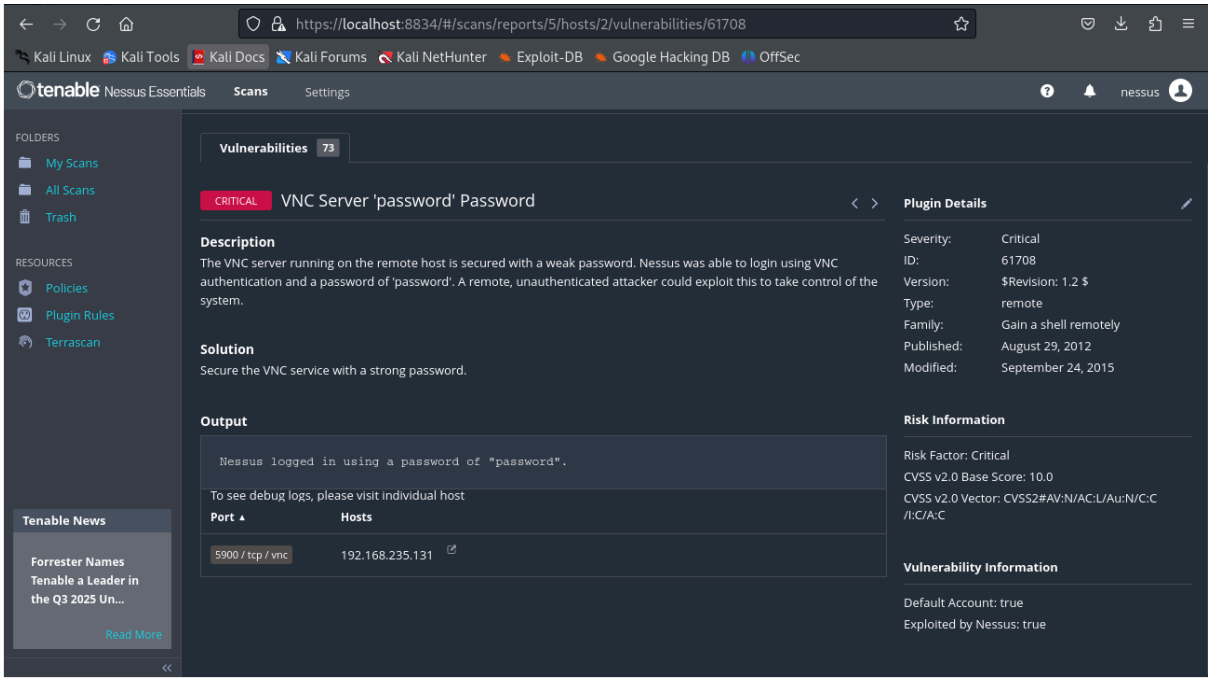
1.port =6667 service =iirc



2.port=80 service=www

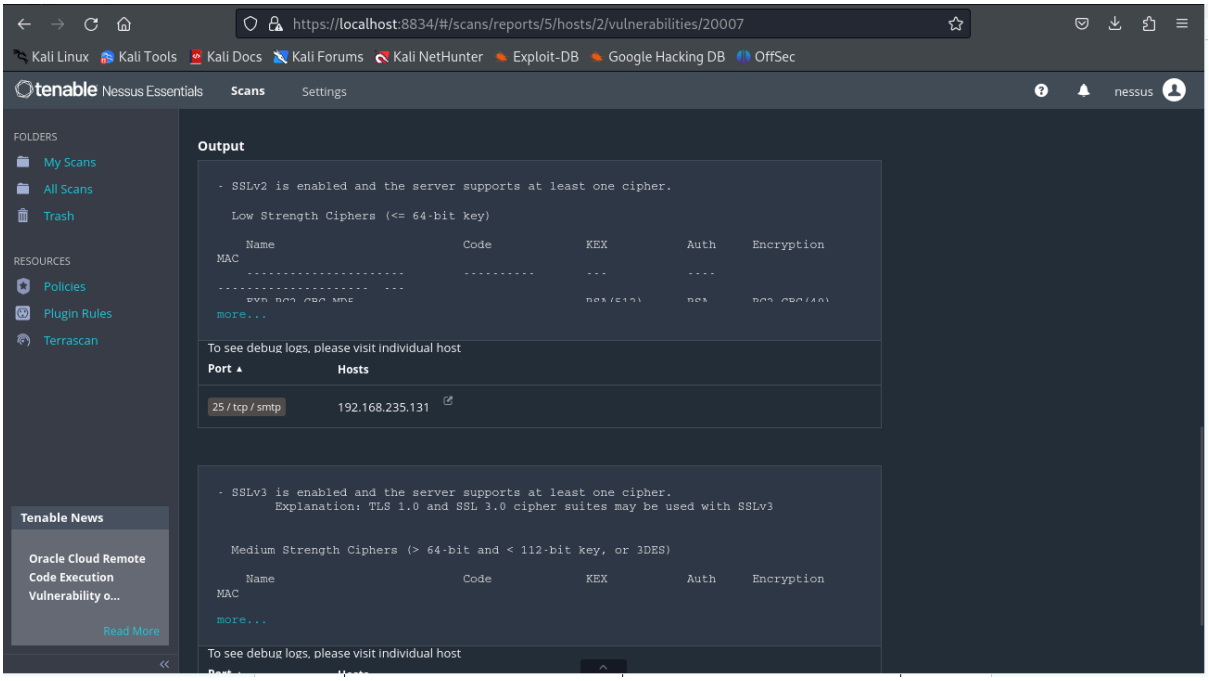


3.port =5900 service=vnc

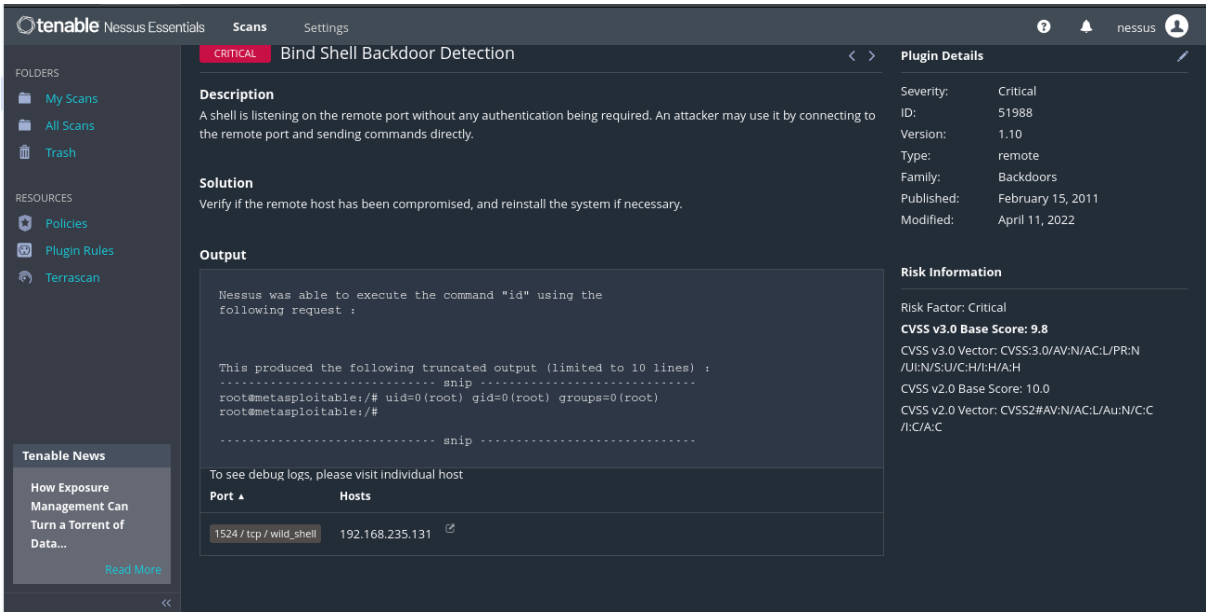


4.port= 25 service=smtp

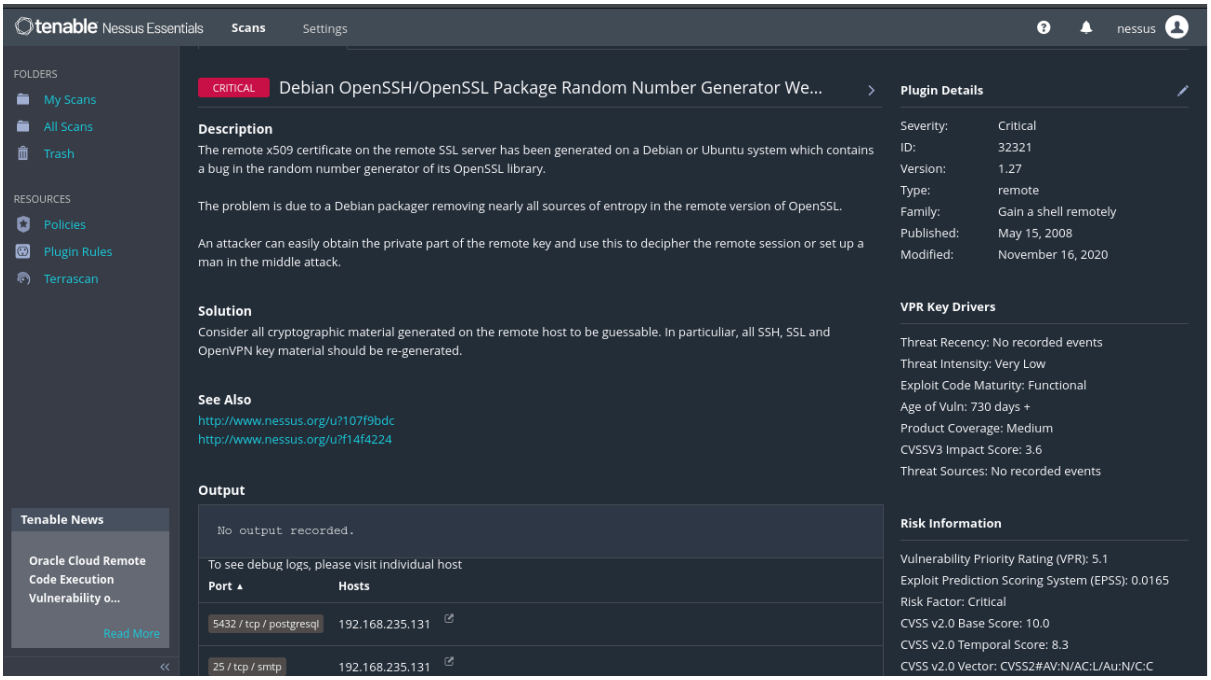
port =5432 service=postgresql



5.port =1524 service=wild_shell



6.port =5432 service= postgresql
port = 25 service=smtp
port = 22 service=ssh



2. เปรียบเทียบผลลัพธ์ที่ได้จากข้อ 1 กับ ที่ได้จาก ZAP

192.168.235.131

9	6	19	8	80
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 122

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	0.9447	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	-	201352	Canonical Ubuntu Linux SEoL (8.04.x)
CRITICAL	10.0*	5.1	0.0165	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0165	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	7.4	0.7216	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

Remote Code Execution - CVE-2012-1823

Source	raised by an active scanner (Remote Code Execution - CVE-2012-1823)
CWE ID	20
WASC ID	20
Reference	• https://owasp.org/www-community/vulnerabilities/Improper_Data_Validation • https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html • https://cwe.mitre.org/data/definitions/89.html

Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	• https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy • https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html • https://www.w3.org/TR/CSP/ • https://w3c.github.io/webappsec-csp/ • https://web.dev/articles/csp • https://caniuse.com/#feat=contentsecuritypolicy • https://content-security-policy.com/

Hidden File Found

Source	raised by an active scanner (Hidden File Finder)
CWE ID	538
WASC ID	13
Reference	• https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html • https://www.php.net/manual/en/function.phpinfo.php

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	• https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
CWE ID	497
WASC ID	13
Reference	• https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework • https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	497
WASC ID	13
Reference	• https://httpd.apache.org/docs/current/mod/core.html#servertokens • https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) • https://www.troyhunt.com/shhh-dont-let-your-response-headers/

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	• https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) • https://owasp.org/www-community/Security_Headers