Vulnerability Assessment

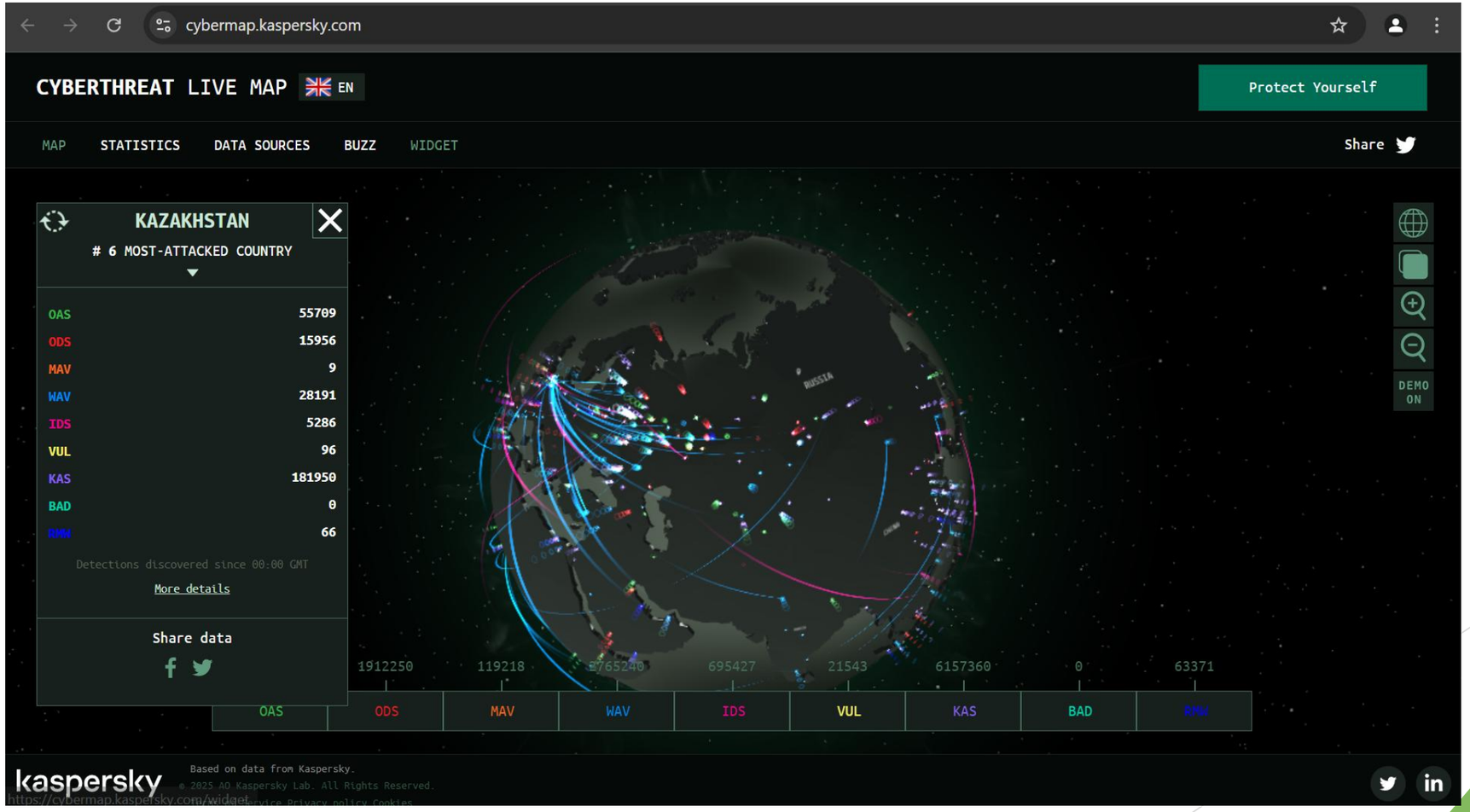
Tenable Nessus

การวิเคราะห์และประเมินจุดอ่อน

ภัยคุกคามทางไซเบอร์

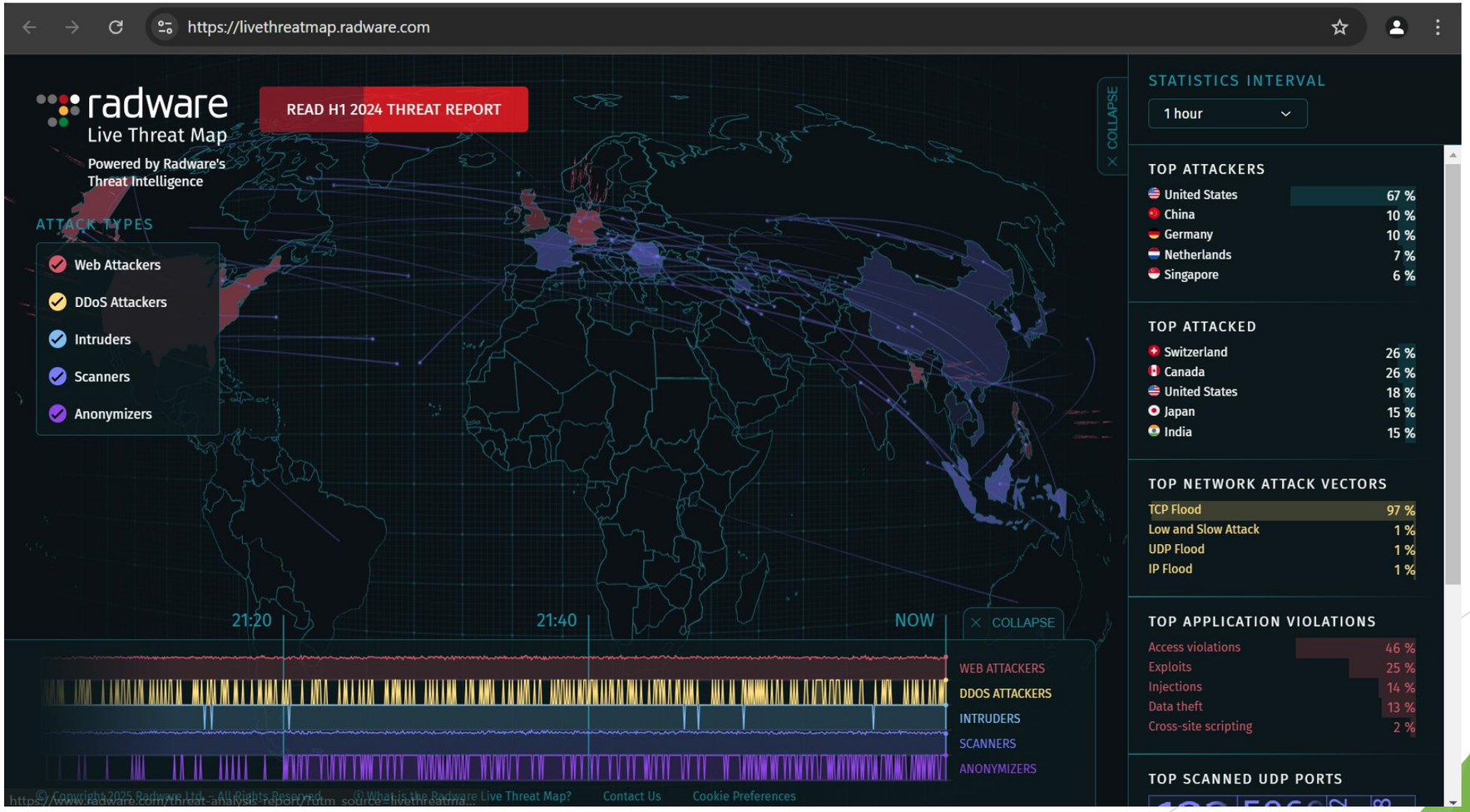
ภัยคุกคามทางไซเบอร์

- https://cybermap.kaspersky.com/



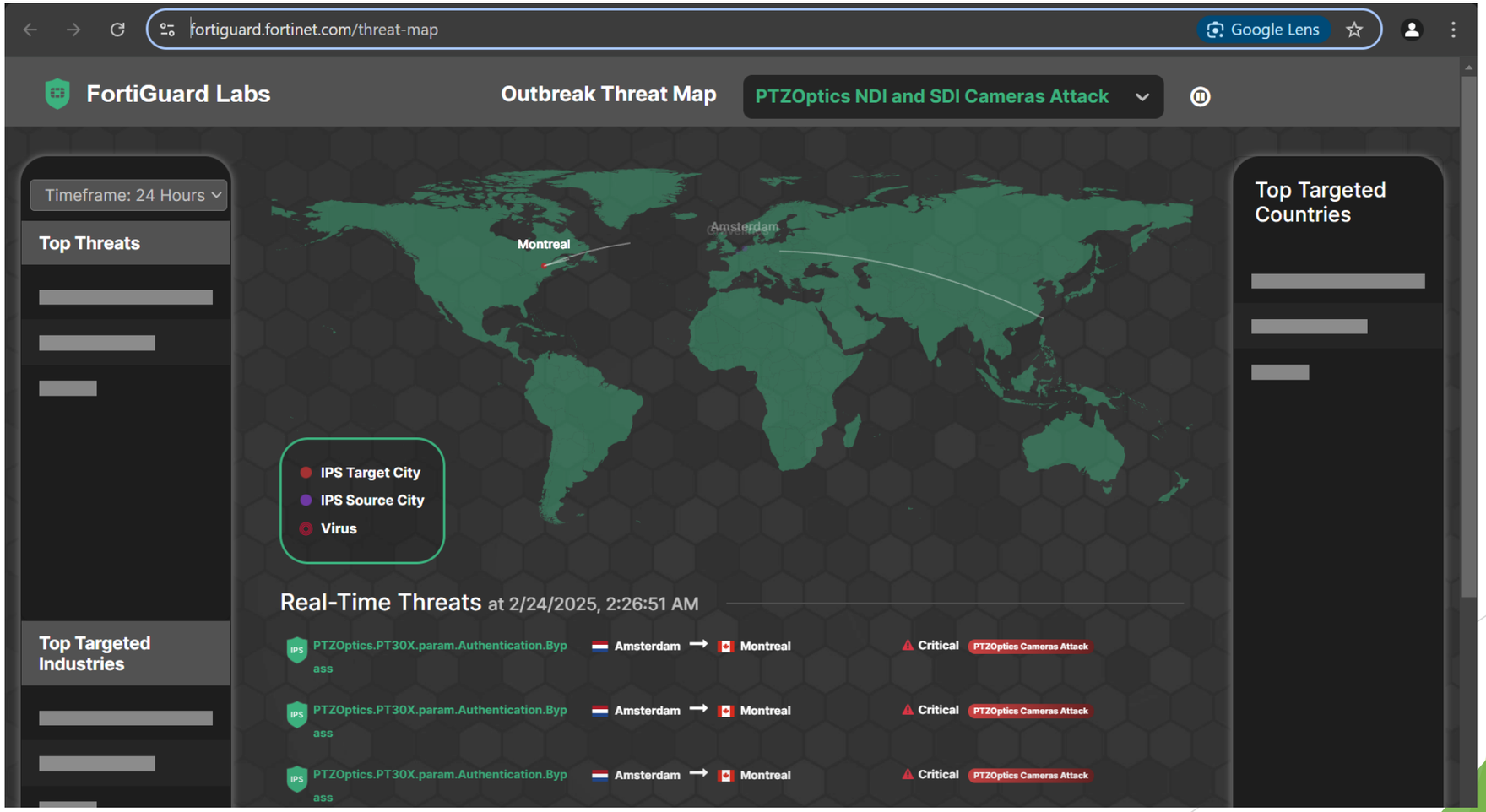
ภัยคุกคามทางไซเบอร์

- https://livethreatmap.radware.com/



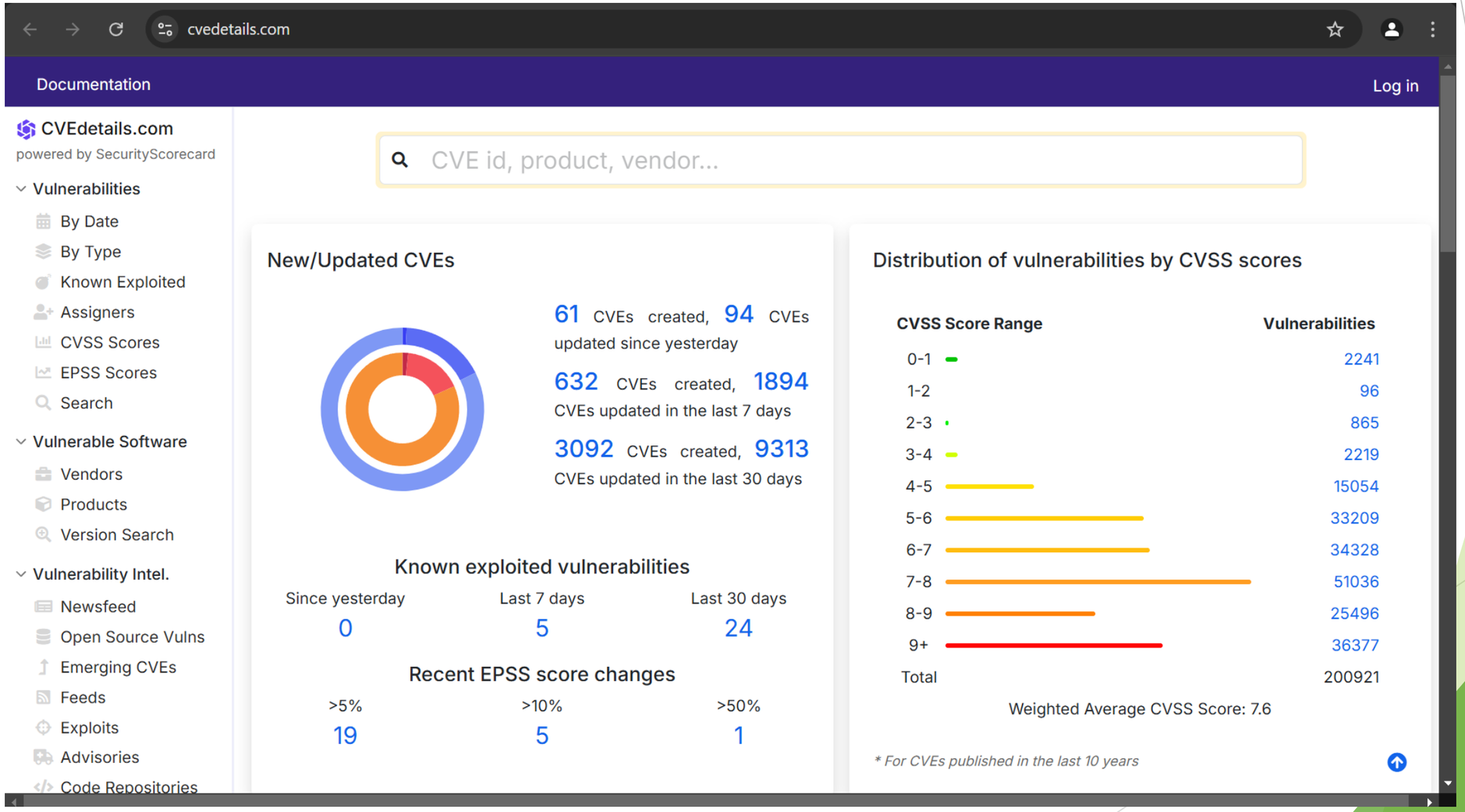
ภัยคุกคามทางไซเบอร์

- https://fortiguard.fortinet.com/threat-map



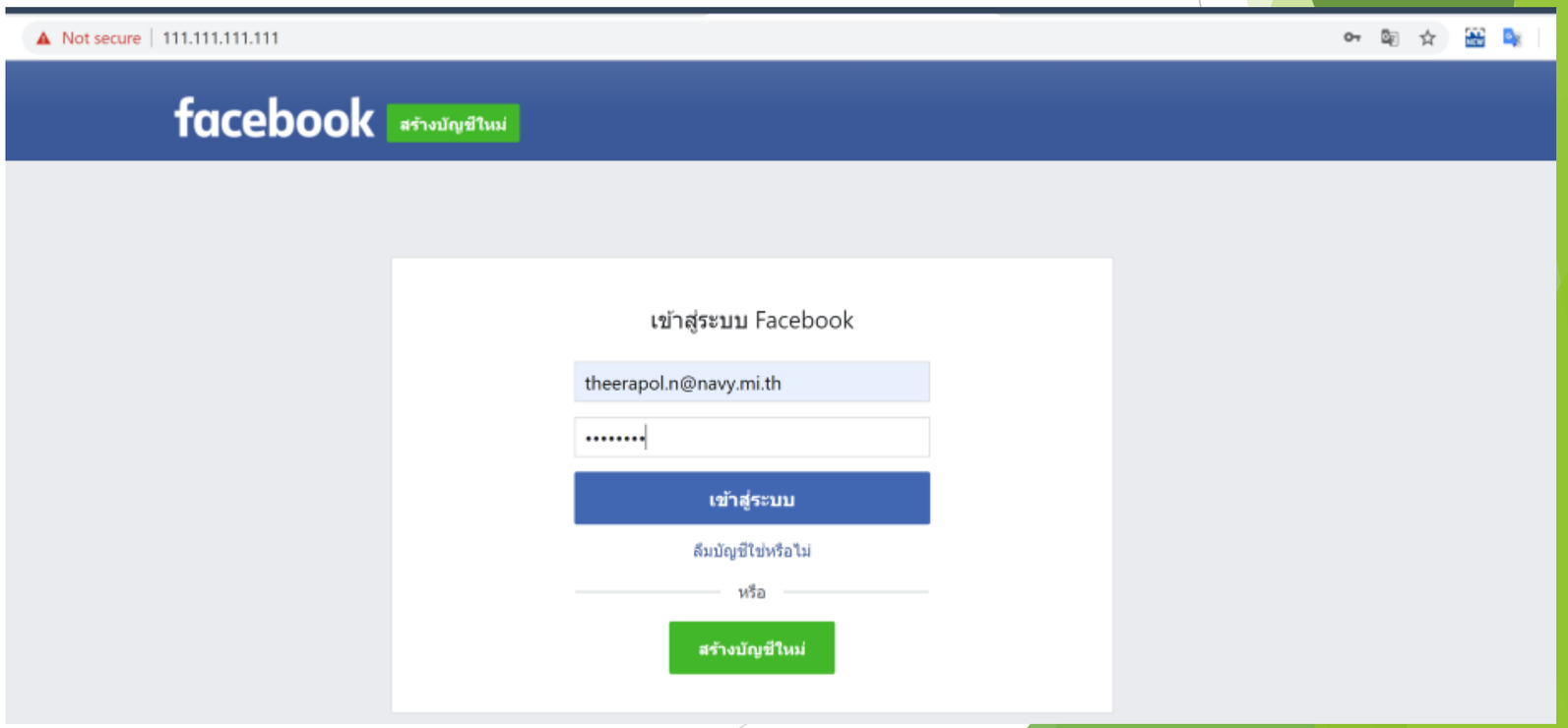
Common Vulnerabilities and Exposures (CVE)

- https://www.cvedetails.com/



ภัยคุกคามทางไซเบอร์

- การหลอกลวงเพื่อเอาข้อมูล
- ขโมยข้อมูล
- เดาสุ่ม
- **เจาะหาช่องโหว่!!!!!!!!!!**



ภาพตัวอย่างการโจมตีจากภายนอกโดยวิธี Injection

#	▼Date/Time	Source Name	Destination	Service	HTTP Host	Action	OWASP Top 10	HTTP URL
1	11:28:54					Alert_Deny	A1:2017-Injection	
2	11:28:54					Alert_Deny	A1:2017-Injection	
3	11:26:59					Alert_Deny	A1:2017-Injection	
4	11:26:59					Alert_Deny	A1:2017-Injection	
5	11:26:53					Alert_Deny	A1:2017-Injection	
6	11:26:53					Alert_Deny	A1:2017-Injection	
7	11:26:46					Alert_Deny	A1:2017-Injection	
8	11:26:46					Alert_Deny	A1:2017-Injection	
9	11:26:45					Alert_Deny	A1:2017-Injection	
10	11:26:45					Alert_Deny	A1:2017-Injection	
11	11:26:42					Alert_Deny	A1:2017-Injection	
12	11:26:42					Alert_Deny	A1:2017-Injection	
13	11:26:40					Alert_Deny	A1:2017-Injection	
14	11:26:40					Alert_Deny	A1:2017-Injection	
15	11:26:38					Alert_Deny	A1:2017-Injection	
16	11:26:38					Alert_Deny	A1:2017-Injection	
17	11:26:36					Alert_Deny	A1:2017-Injection	
18	11:26:36					Alert_Deny	A1:2017-Injection	
19	11:26:35					Alert_Deny	A1:2017-Injection	
20	11:26:35					Alert_Deny	A1:2017-Injection	
21	11:26:33					Alert_Deny	A1:2017-Injection	

ความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ป้องกันการเข้าถึงข้อมูลและระบบของธุรกิจจากผู้ไม่ประสงค์ดี ซึ่งอาจส่งผลกระทบร้ายแรงต่อการดำเนินงานและชื่อเสียง

สร้างความไว้วางใจและความมั่นใจให้กับลูกค้า พนักงาน และหุ้นส่วนของธุรกิจ ในการรับมอบความรับผิดชอบในการปกป้องข้อมูลที่สำคัญ

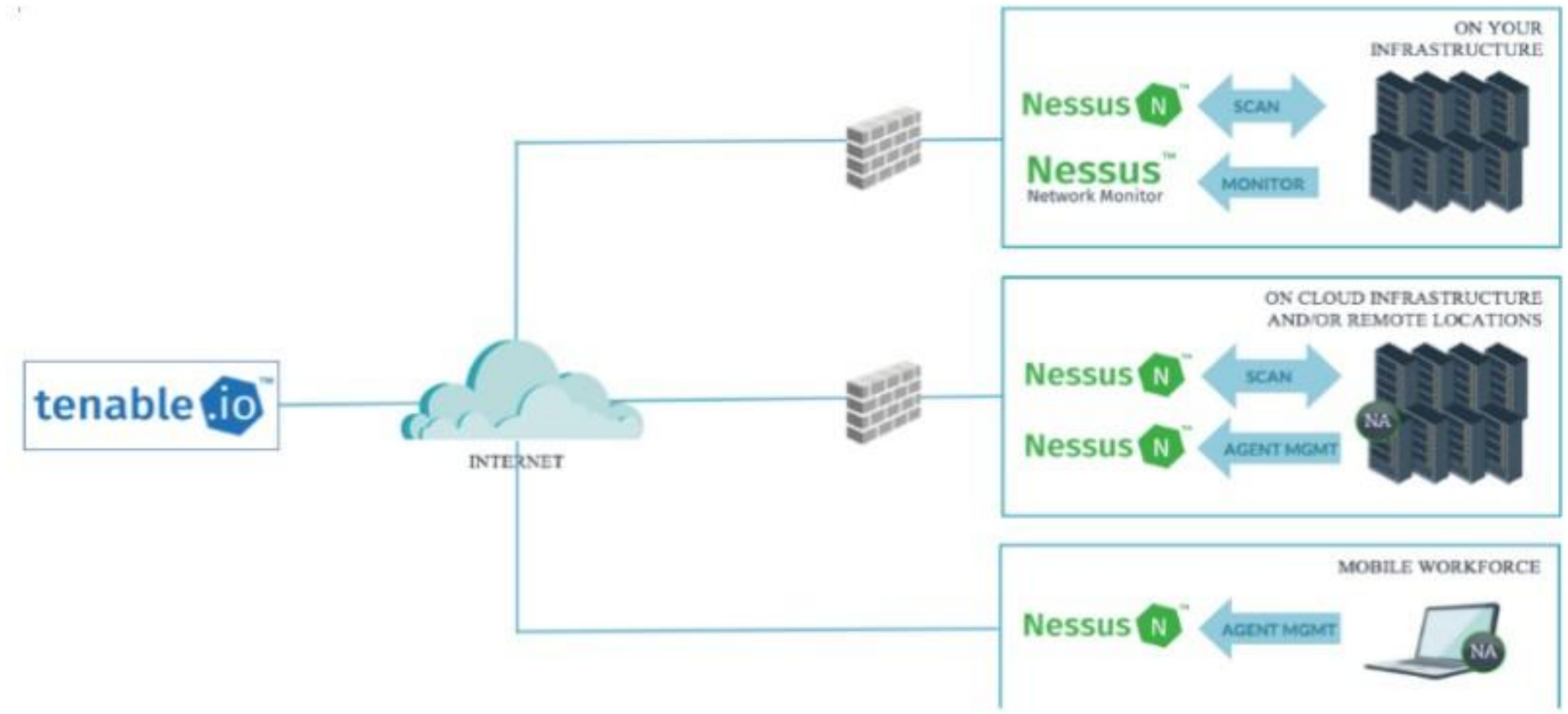
ความรู้เบื้องต้นเกี่ยวกับโปรแกรม Nessus

- Nesses เป็นโปรแกรมฟรีและเปิดรหัสสำหรับการตรวจหาช่องโหว่ในระบบเครือข่ายและไอที
- โปรแกรมนี้ใช้หลักการและอัลกอริทึมขั้นสูงในการค้นหาจุดอ่อนด้านความปลอดภัยในระบบคอมพิวเตอร์
- Nexes สามารถตรวจพบช่องโหว่ด้านรหัสโปรแกรมและการตั้งค่าระบบไอทีต่างๆ เพื่อปรับปรุงให้มั่นคงยิ่งขึ้น

License Comparison

	Nessus Essentials	Nessus Professional	Nessus Expert
เหมาะกับใคร	การเรียนรู้/ฝึกฝน การฝึกอบรม (การใช้งานที่ไม่ใช่เชิงพาณิชย์)	ที่ปรึกษาด้านความปลอดภัย องค์กรหรือทีมไอที ที่ต้องการการประเมินความปลอดภัยภายใน (Internal Threats) อย่างครอบคลุม	หน่วยงานหรือองค์กรขนาดใหญ่ที่ต้องการการประเมินความปลอดภัยขั้นสูง (Internal & External Threats, Cloud)
การจำกัด IP	16 IP	ไม่จำกัด	ไม่จำกัด
ราคา	ฟรี	~160,490 บาท / ปี	~ 241,810 บาท / ปี
External Attack Surface Management	✕	✕	✓
Cloud Infrastructure Assessment	✕	✕	AWS / Azure / GCP
Container Security	✕	✕	✓
ประเภทการสแกน	Credentialed & non-credentialed scans	Credentialed & non-credentialed Custom scans	Credentialed & non-credentialed Custom scans Cloud & external scans
Reporting & Analysis	Basic reports (CSV, HTML, PDF)	Advanced reporting, customizable reports	Advanced reporting including cloud and external attack surface
Integration & Automation	Limited or no advanced integrations	API support for automation & integration	API support, plus cloud and external management
Support	Community support	Standard support included Portal Support Chat Support	Premium support available Portal Support Chat Support Phone Support Direct access & Fully supported by team of Tier II Engineers

Diagram


tenable.io
INTERNET
ON YOUR INFRASTRUCTURE
Nessus
SCAN
Nessus
Network Monitor
MONITOR
ON CLOUD INFRASTRUCTURE AND/OR REMOTE LOCATIONS
Nessus
SCAN
NA
Nessus
AGENT MGMT
MOBILE WORKFORCE
Nessus
AGENT MGMT
NA

Hardware Requirements

Essential

2 Cores (Minimum)

4 Cores (**Recommended**)

4 GB (Minimum)

8 GB (**Recommended**)

30 GB (Minimum)

50 GB SSD (**Recommended**)

1 Gbps

Professional & Expert

4(2GHz) Cores (**50,000 Host / Scan**)

4(2GHz) Cores or higher (**>50,000 Host / Scan**)

8(2GHz) Cores or higher (**Web App Scan**)

4 GB (**50,000 Host / Scan**)

8 GB or higher (**>50,000 Host / Scan, Web App Scan**)

30 GB (**50,000 or more Host / Scan**)

40 GB (**Web App Scan**)

1 Gbps

วิธีติดตั้งและใช้งานโปรแกรม Nessus

1

ดาวน์โหลดโปรแกรม

ดาวน์โหลดโปรแกรม Nessus จากเว็บไซต์

2

ติดตั้งโปรแกรม

ติดตั้งโปรแกรมลงในเครื่องคอมพิวเตอร์
หรือเครื่องคอมพิวเตอร์แม่ข่ายที่ต้องการตรวจสอบ

3

เริ่มใช้งาน

เมื่อติดตั้งเสร็จ เปิดใช้งานเพื่อเริ่มเริ่มสแกนค้นหาช่องโหว่ในระบบ

ขั้นตอนการตรวจสอบช่องโหว่เบื้องต้น

1

เลือกประเภทของระบบและเครือข่าย

เลือกประเภทของระบบและเครือข่ายที่ต้องการตรวจสอบ เช่น เว็บแอปพลิเคชัน, เซิร์ฟเวอร์, เครือข่ายไร้สาย

2

กำหนดขอบเขตและมุมมองในการตรวจสอบ

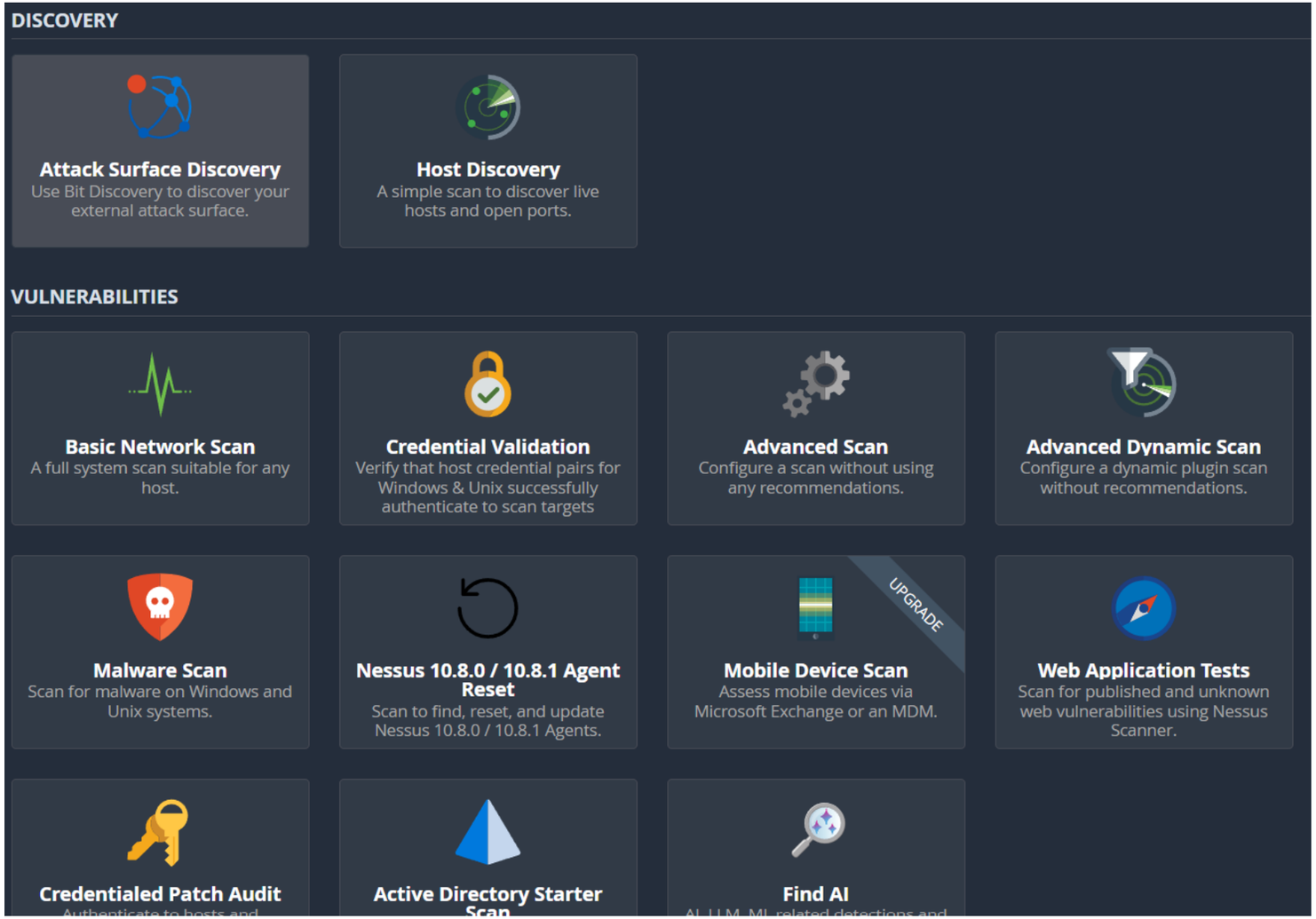
กำหนดขอบเขตและมุมมองในการตรวจสอบ เพื่อให้ครอบคลุมทั้งระบบและเชื่อมโยงกันได้อย่างมีประสิทธิภาพ

3

เริ่มทำการสแกนด้วยโปรแกรม Nessus

เริ่มทำการสแกนด้วยโปรแกรม Nexes โดยปฏิบัติตามขั้นตอนอย่างถูกต้อง เพื่อค้นหาจุดอ่อนที่อาจเป็นช่องโหว่

Categories


DISCOVERY
Attack Surface Discovery
Use Bit Discovery to discover your external attack surface.
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Nessus 10.8.0 / 10.8.1 Agent Reset
Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.
UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Active Directory Starter Scan
Find AI

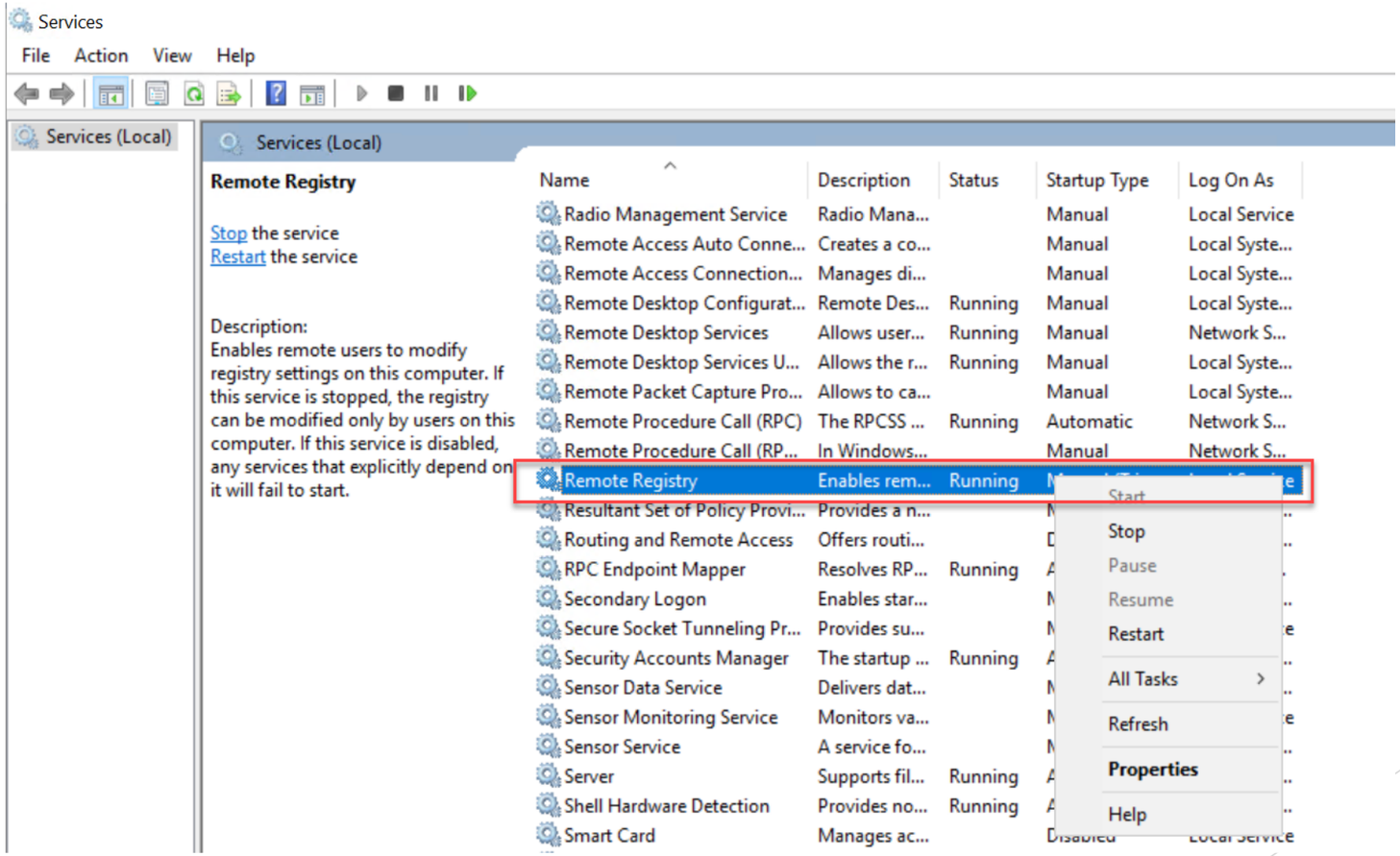
Scan Requirements

- ก่อนเริ่มทำการสแกนด้วย Nessus Expert มี Requirements ที่ใช้ในการสแกน ดังนี้

1. **Credentials** ที่ใช้ในการสแกนอุปกรณ์ปลายทาง ต้องเป็นสิทธิ์สูงสุด เช่น Administrator (Windows) , root (Linux)

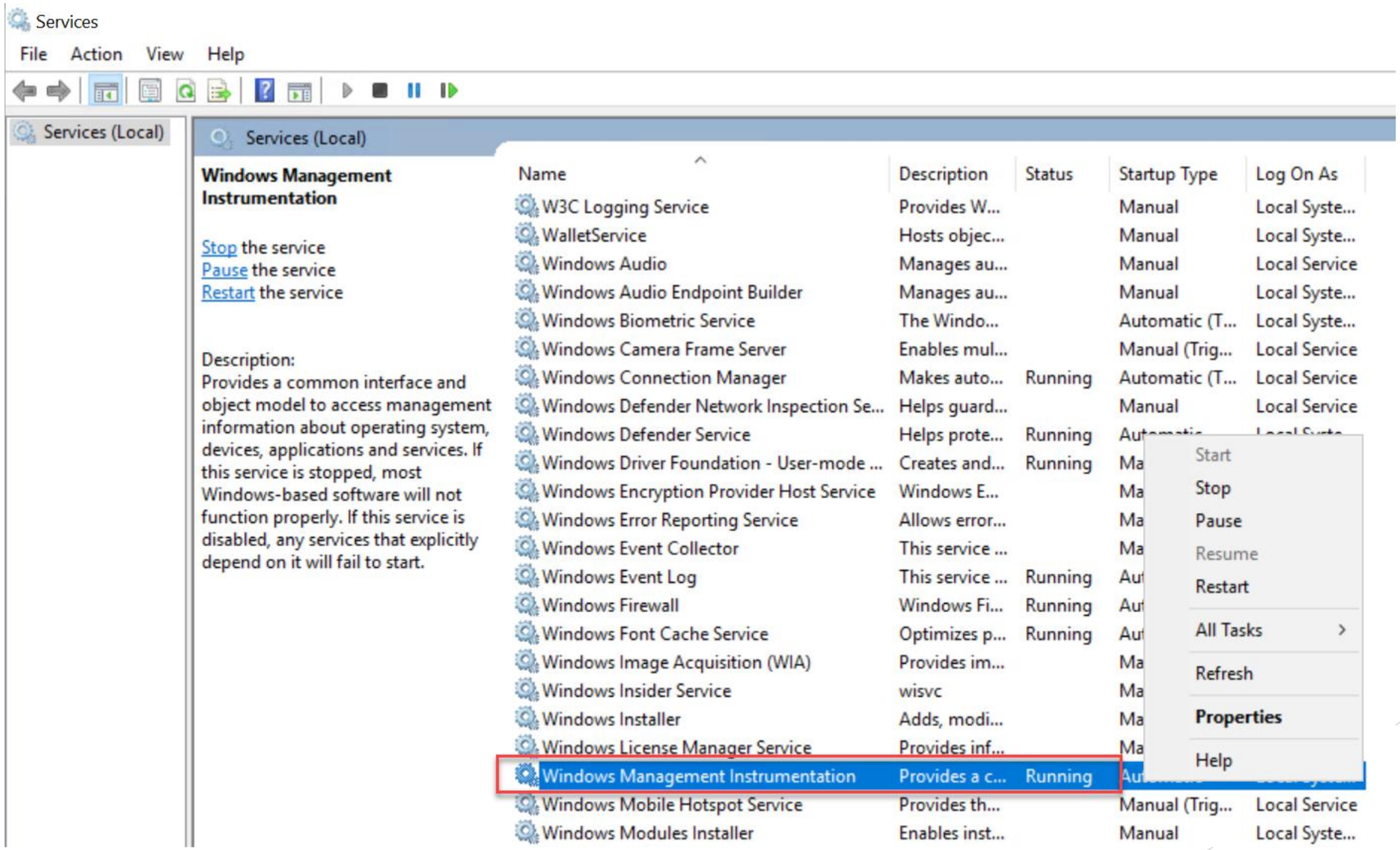
2. การสแกนเครื่องที่เป็น Windows จำเป็นต้องเปิด Service เหล่านี้

2.1 **Service Remote Registry** โดยไปที่ **Services > Remote Registry > Start**



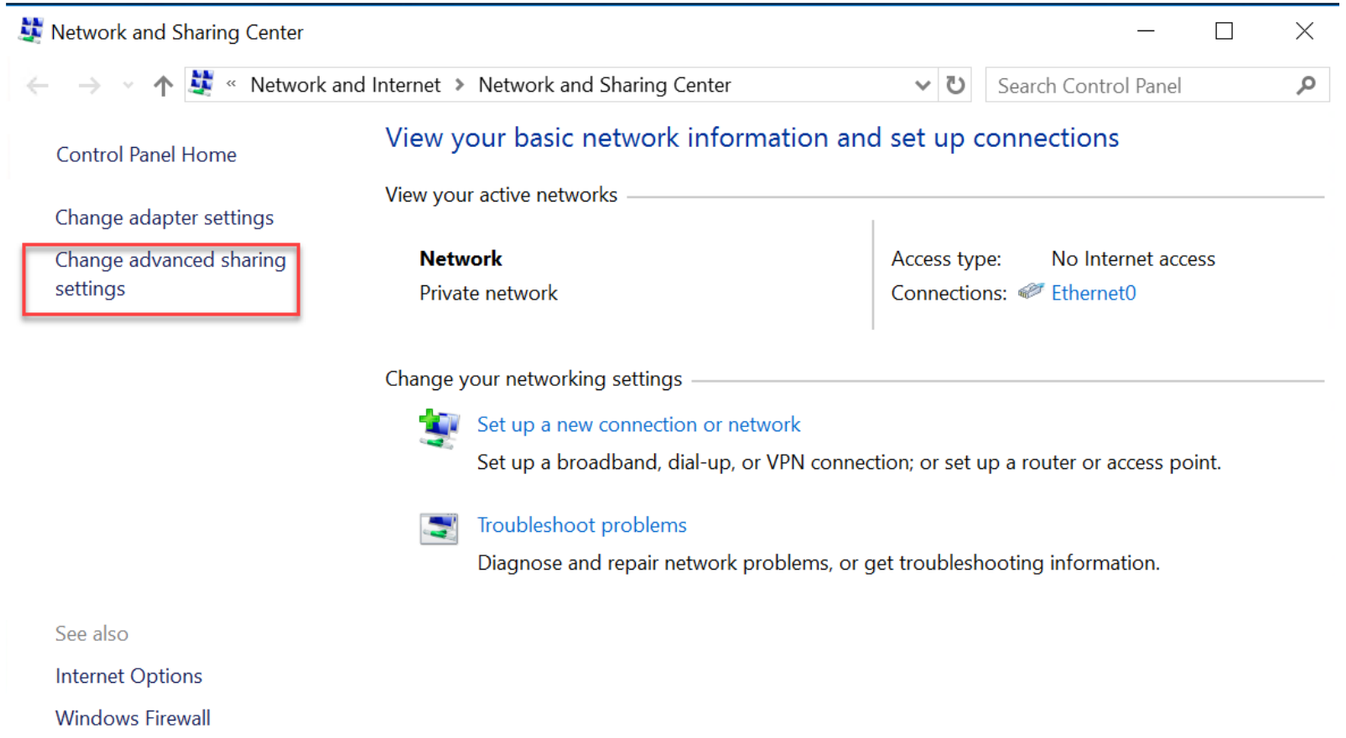
Scan Requirements

2.2 **Service WMI** โดยไปที่ **Services > Windows Management Instrumentation > Start**



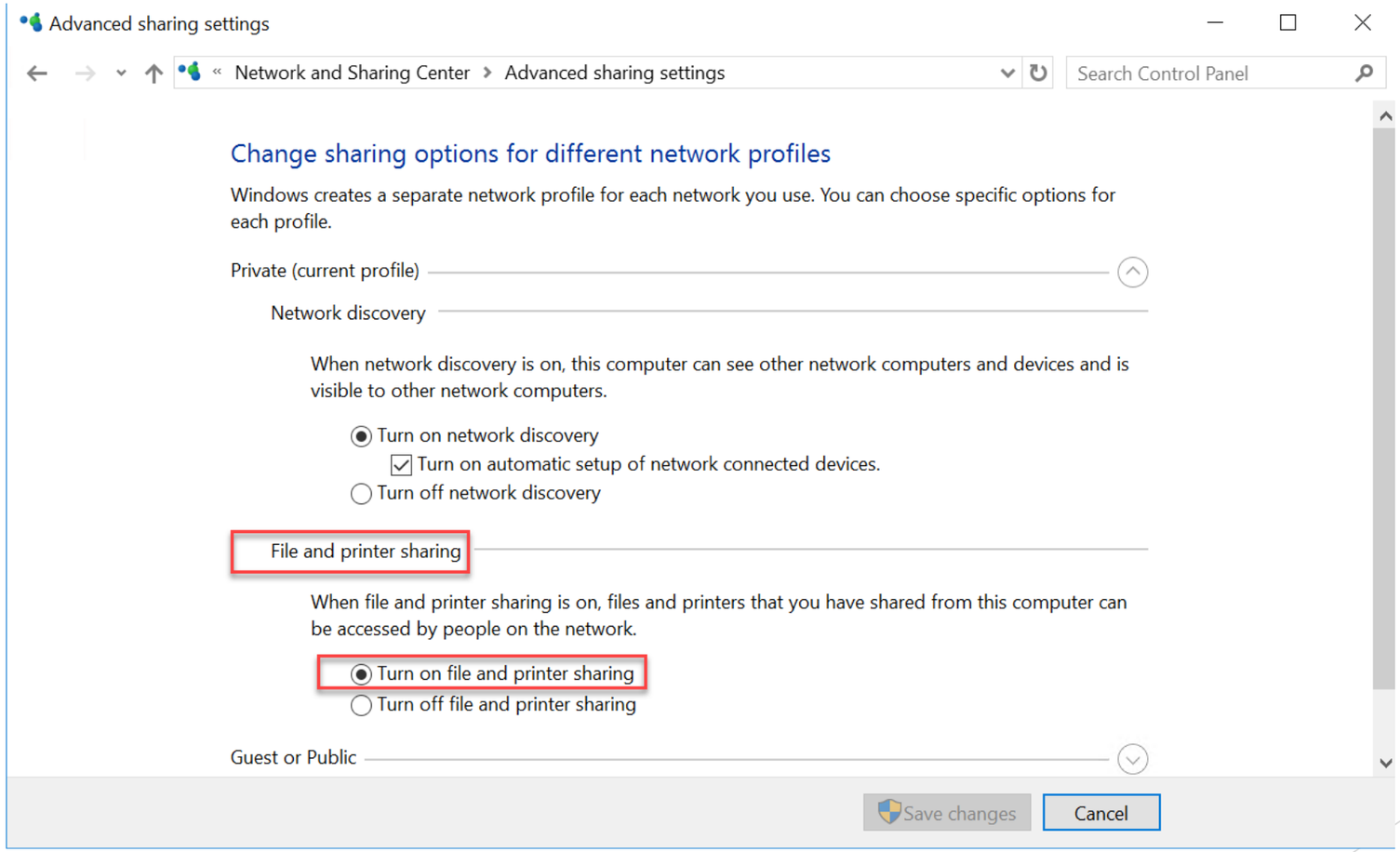
Scan Requirements

2.3 File Sharing and Printer ไปที่ Network and Sharing Center > Change advance sharing setting



Scan Requirements

จากนั้นไปที่ **File and Printer sharing** ทำการเลือกที่ **Turn on file and printer sharing** จากนั้นกด **save changes**

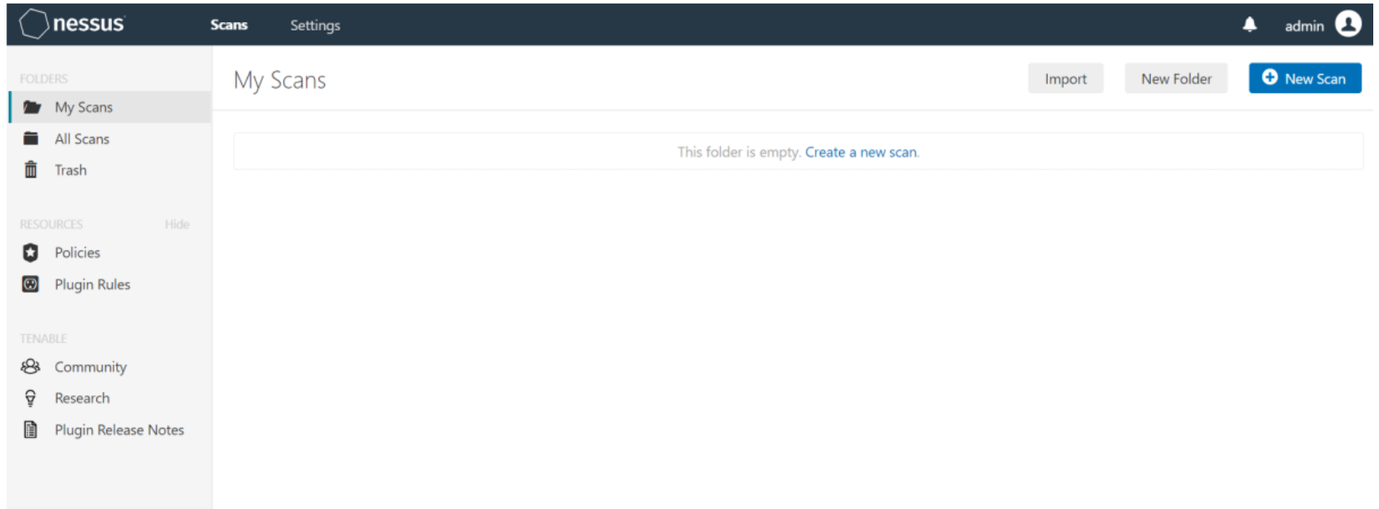


Create Scan

กดที่ปุ่ม สีน้ำเงินที่ชื่อว่า **New Scan** เพื่อสร้าง **Policy** สำหรับการสแกน

จากนั้นจะปรากฏหน้าของ **Policy Template** ขึ้นมาให้เลือกใช้งาน

โดยปกติ **Policy Template** หลักๆ ที่ใช้งานจะมีอยู่ 2 ตัวด้วยกัน คือ **Host Discovery** กับ **Basic Network**

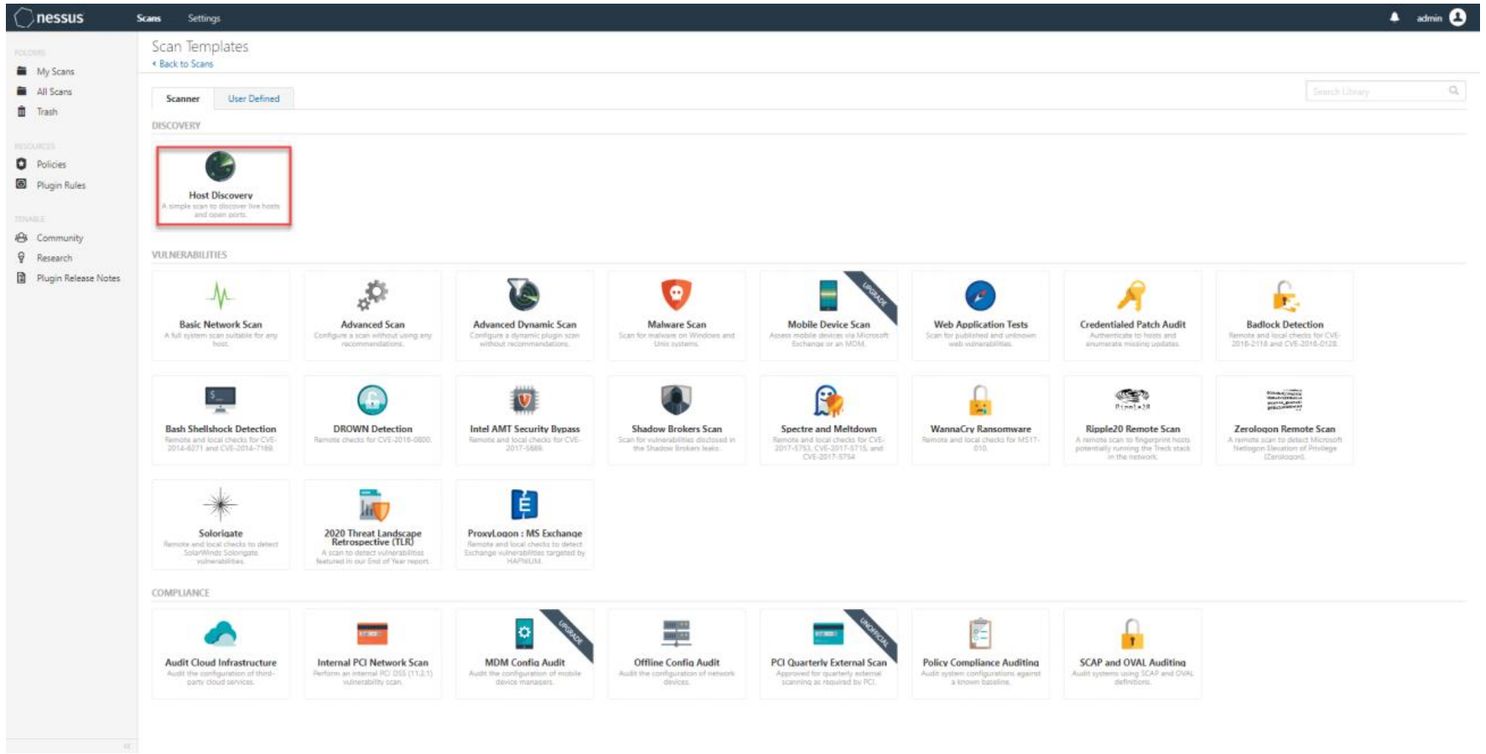


Create Scan

Host Discovery

จะเป็นการสแกนหา IP ของเครื่องที่กำลัง Online อยู่ในองค์กร ณ ขณะนั้น ลักษณะการสแกนจะเป็นการ Ping ไปที่เครื่องปลายทาง หากเครื่องปลายทางมีการตอบสนองกลับมาแปลว่าสแกนเจอเครื่องปลายทางเหล่านั้น โดย Policy ตัวนี้จะมีการสแกนที่ไวกว่า Policy ตัวอื่นๆเนื่องจากใช้ Pluginที่เกี่ยวกับการค้นหาอุปกรณ์ปลายทางโดยเฉพาะ

Create Scan


nessus
Scans
Settings
admin
My Scans
All Scans
Trash
Policies
Plugin Rules
Community
Research
Plugin Release Notes
Scan Templates
Back to Scans
Scanner
User Defined
DISCOVERY
Host Discovery
VULNERABILITIES
Basic Network Scan
Advanced Scan
Advanced Dynamic Scan
Malware Scan
Mobile Device Scan
Web Application Tests
Credentialed Patch Audit
Badlock Detection
Bash Shellshock Detection
DROWN Detection
Intel AMT Security Bypass
Shadow Brokers Scan
Spectre and Meltdown
WannaCry Ransomware
Ripple20 Remote Scan
Zerologon Remote Scan
Solorigate
2020 Threat Landscape Retrospective (TLR)
ProxyLogon : MS Exchange
COMPLIANCE
Audit Cloud Infrastructure
Internal PCI Network Scan
MDM Config Audit
Offline Config Audit
PCI Quarterly External Scan
Policy Compliance Auditing
SCAP and OVAL Auditing

Create Scan

จากนั้นทำการใส่ข้อมูลในกรอบสีแดง

Name : ชื่อ Policy Scan ที่ต้องการตั้ง

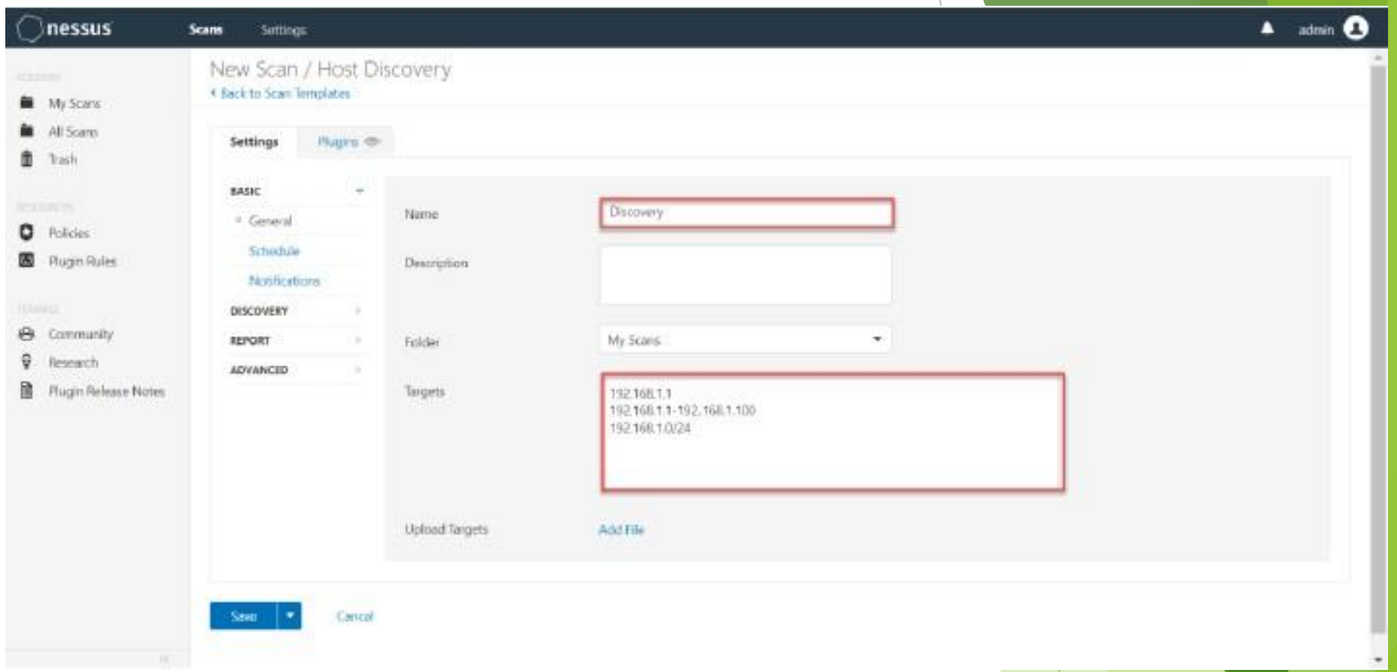
Target : ระบุเครื่องที่ต้องการสแกนด้วย IP Address ตามที่ต้องการ

โดยวิธีการระบุ IP สามารถระบุได้หลายแบบ เช่น

ทำการสแกน IP เดียว เช่น 192.168.1.1

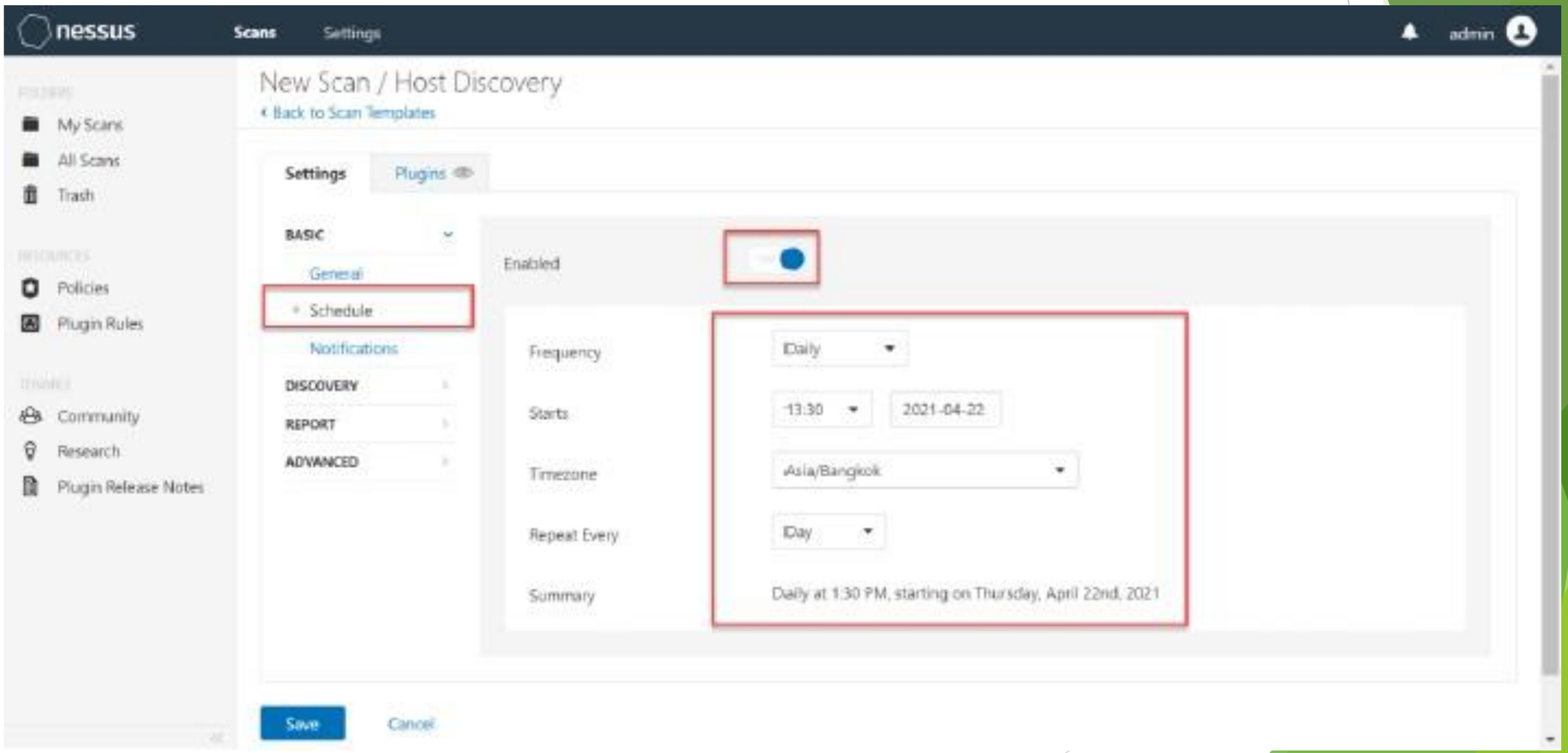
ทำการสแกน IP ตั้งแต่ 1 ถึง 100 เช่น 192.168.1.1-192.168.1.100

ทำการสแกน IP เป็น Class Range เช่น 192.168.1.0/24



Create Scan

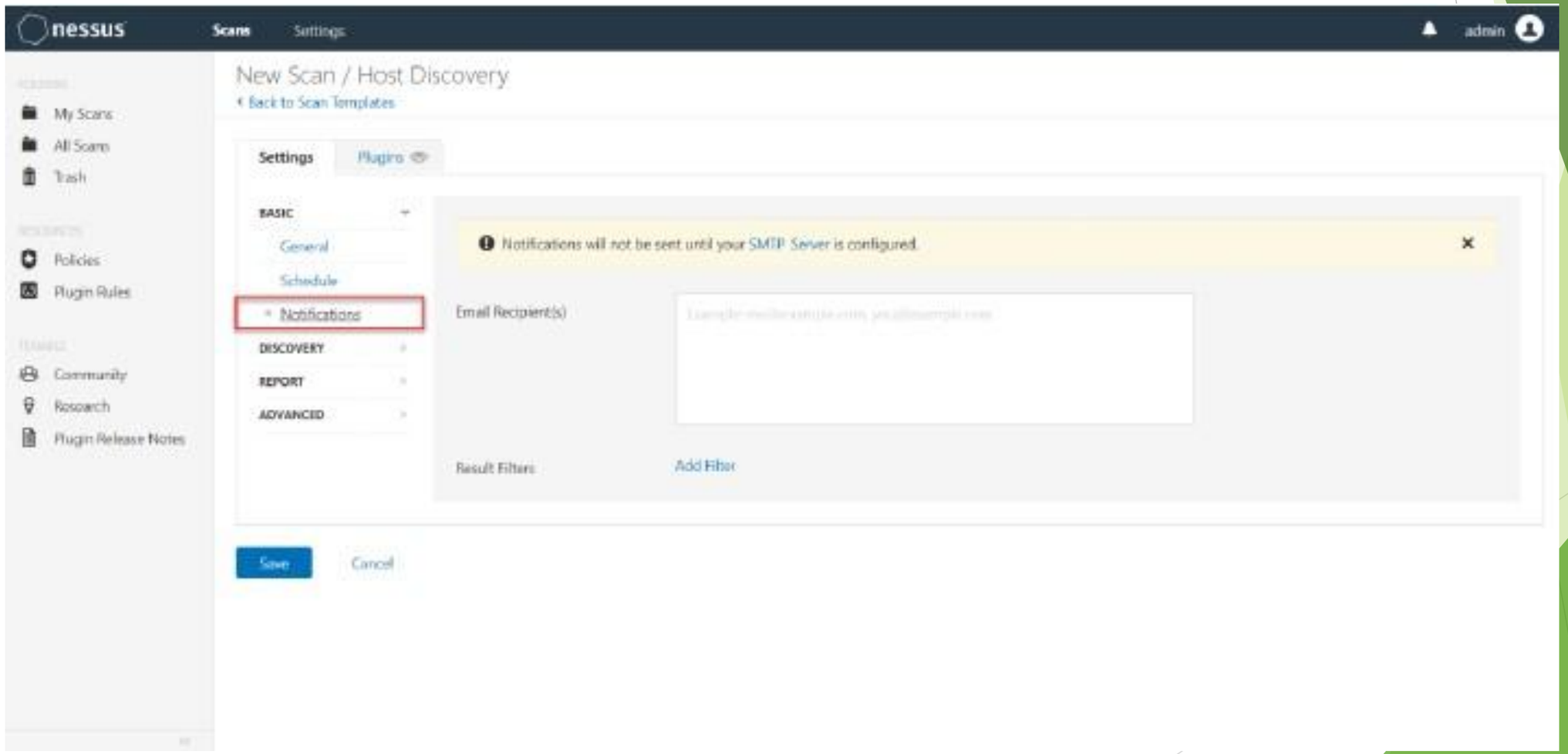
สามารถตั้ง **Schedule** ในการสแกนเป็น **Daily** , **Weekly** หรือ **Monthly** ได้



Create Scan

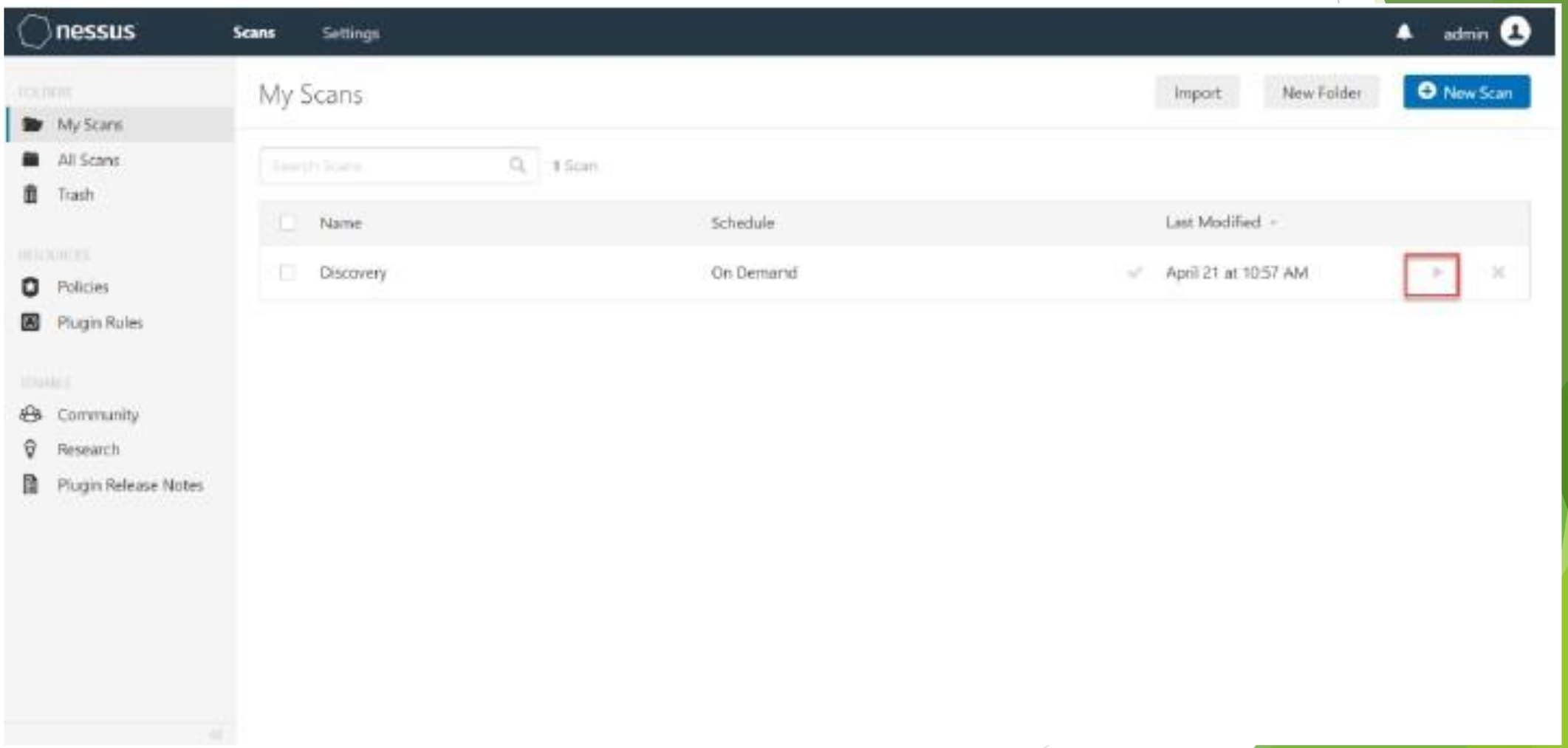
สามารถตั้ง **Notifications** แจ้งเตือนทาง **Email** หลังจากทำการสแกนเสร็จ โดยไม่จำเป็นเชื่อมต่อกับ **SMTP Server**

จากนั้นทำการกดปุ่ม Save เป็นอันเสร็จ



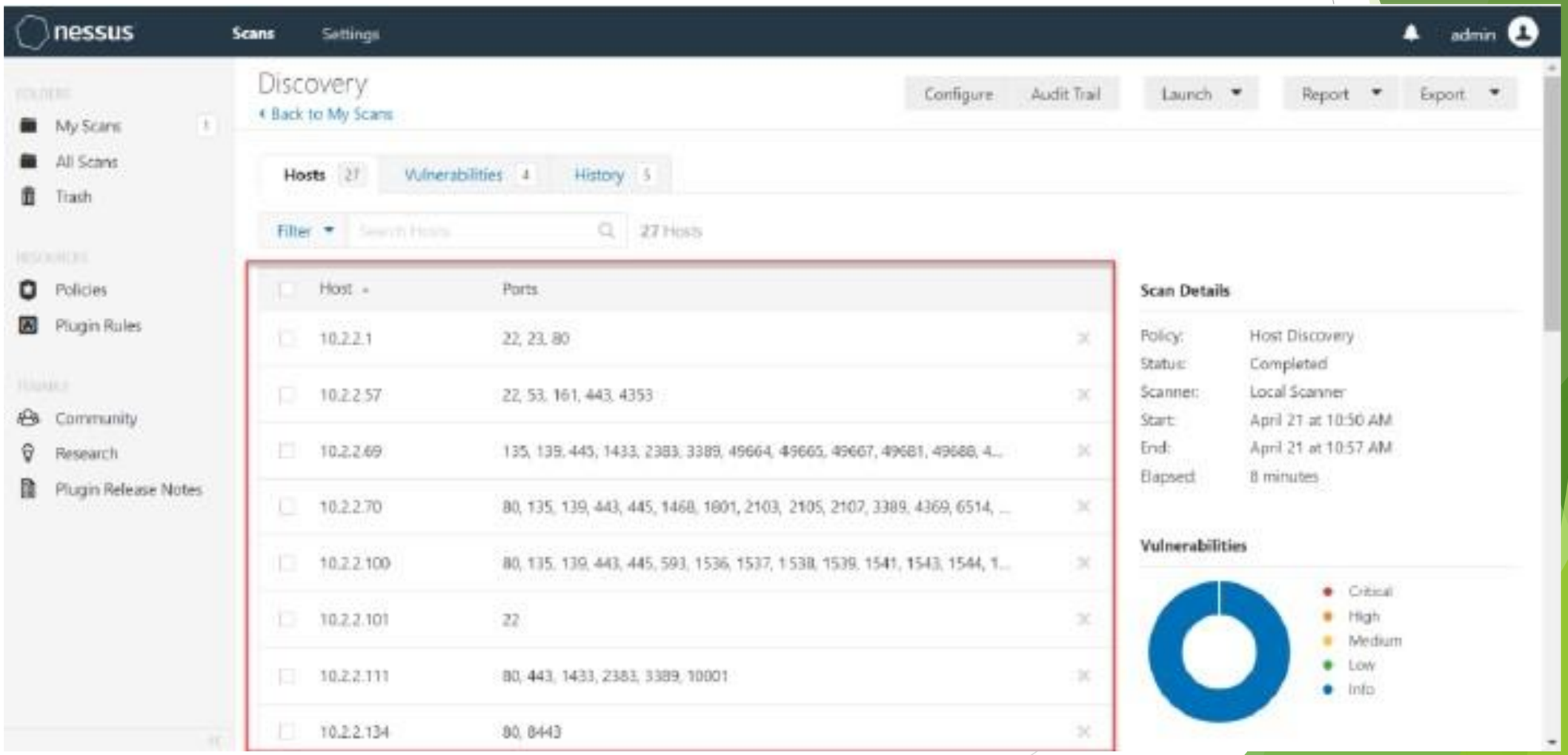
Create Scan

จะปรากฏ **Policy** ที่ใช้สำหรับการสแกนขึ้นมา จากนั้นทำการกดที่**ปุ่มสามเหลี่ยม**ในกรอบสีแดง เพื่อทำการสั่งสแกน



Create Scan

ผลลัพธ์จะแสดงเกี่ยวกับเครื่องที่เจอ รวมถึง port ที่เปิดอยู่ของเครื่องนั้นๆ



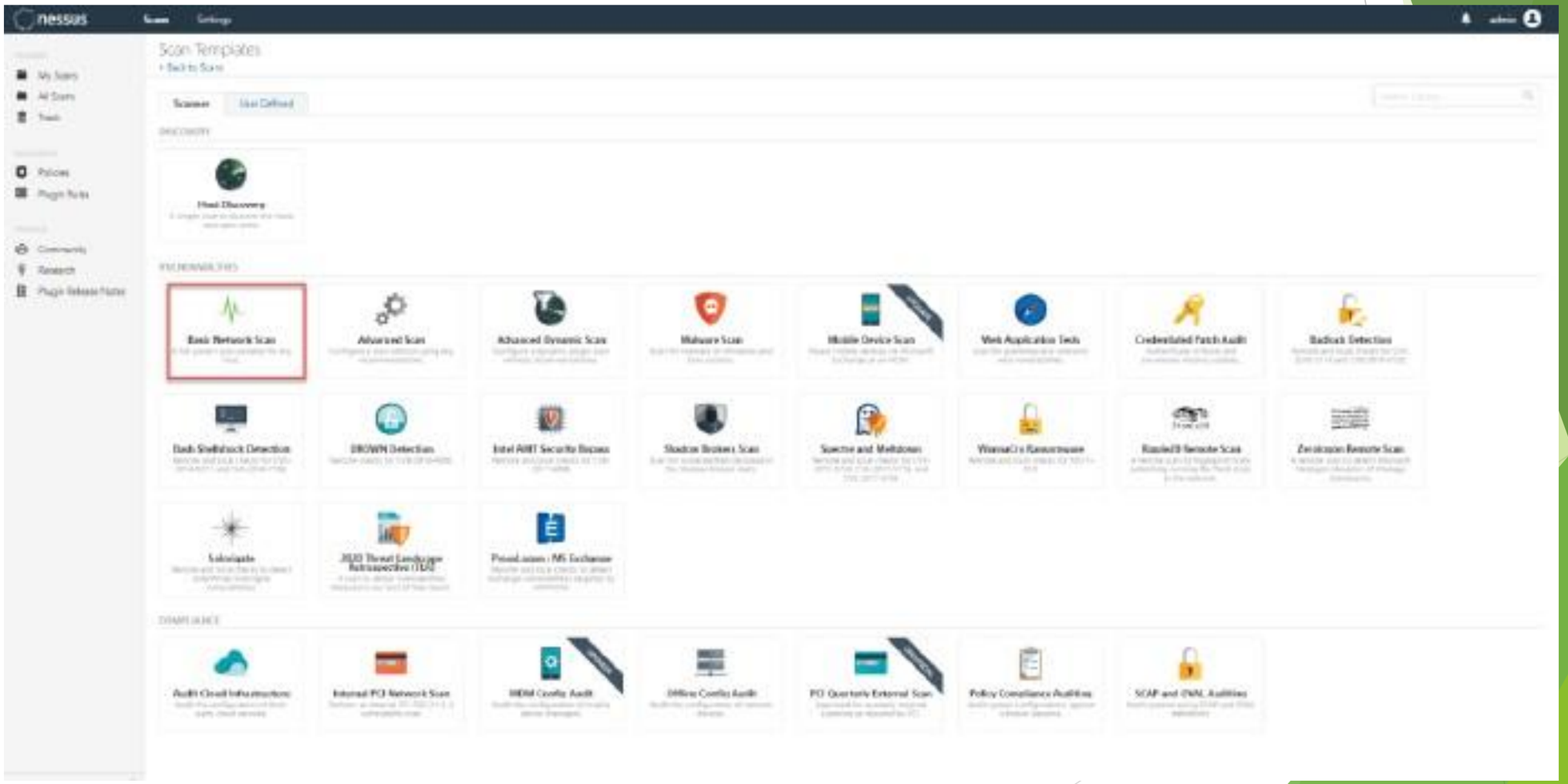
Create Scan

Basic Network Scan

จะเป็นการเข้าไปสแกนในเครื่องปลายทาง โดยทำการหาช่องโหว่ต่างๆ
ของเครื่องปลายทางที่เข้าไปทำการสแกน โดยจำเป็นต้องการตัว Credential ของเครื่องปลายทาง
และจำเป็นต้องมีสิทธิ์สูงสุด เช่น Administrator (Windows) , root (Linux)
โดยตัว Basic Network Scan จะเป็นการสแกนแบบใช้ Plugin ทั้งหมดที่มี
ของตัว Nessus Expert ซึ่งการสแกนแบบนี้จะง่ายต่อการใช้งาน

Create Scan

ต้องการสแกนหาช่องโหว่ของอุปกรณ์ เลือก **Basic Network Scan**



Create Scan

จากนั้นทำการใส่ข้อมูลในกรอบสีแดง

Name : ชื่อ Policy Scan ที่ต้องการตั้ง

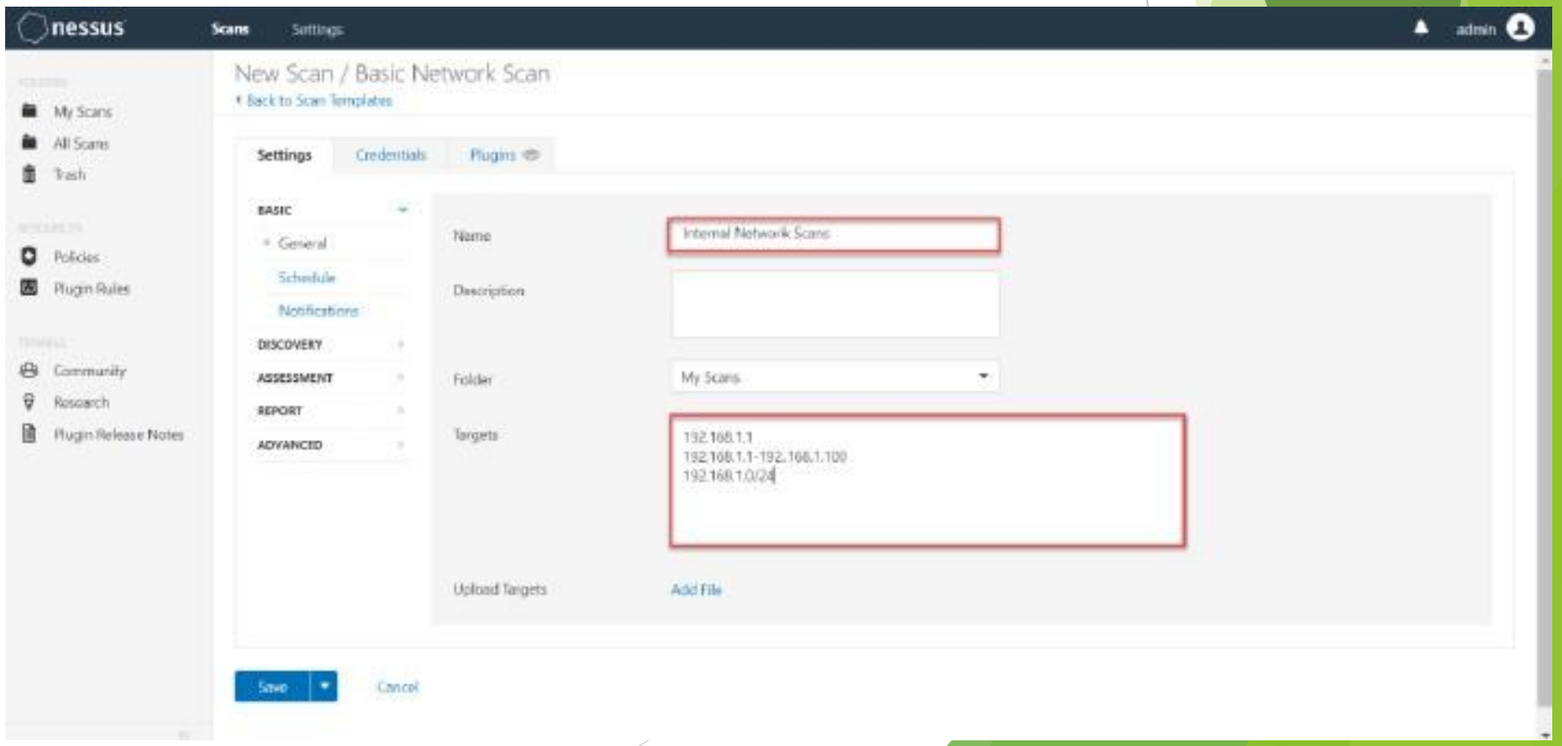
Target : ระบุเครื่องที่ต้องการสแกนด้วย IP Address ตามที่ต้องการ

โดยวิธีการระบุ IP สามารถระบุได้หลายแบบ เช่น

ทำการสแกน IP เดียว เช่น 192.168.1.1

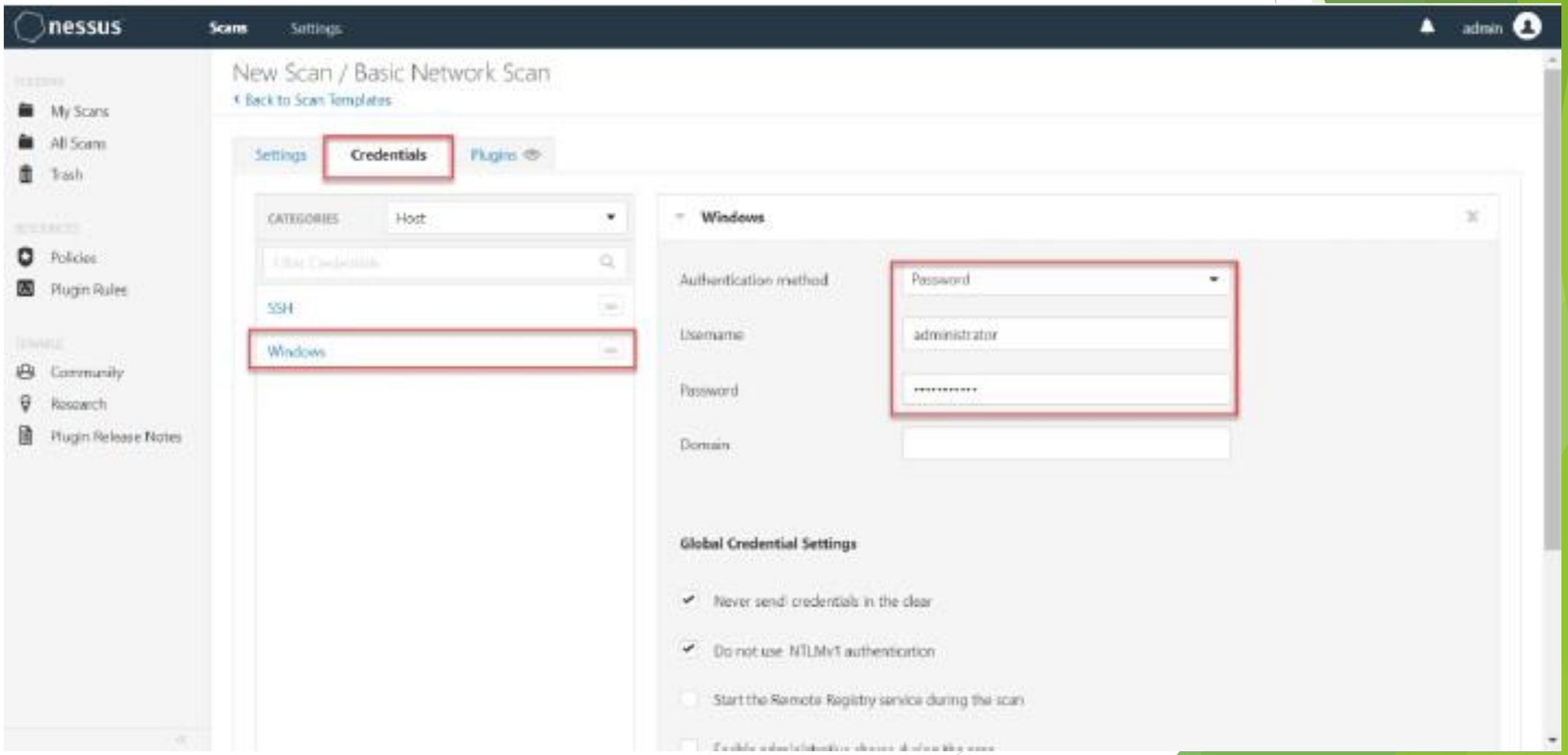
ทำการสแกน IP ตั้งแต่ 1 ถึง 100 เช่น 192.168.1.1-192.168.1.100

ทำการสแกน IP เป็น Class Range เช่น 192.168.1.0/24



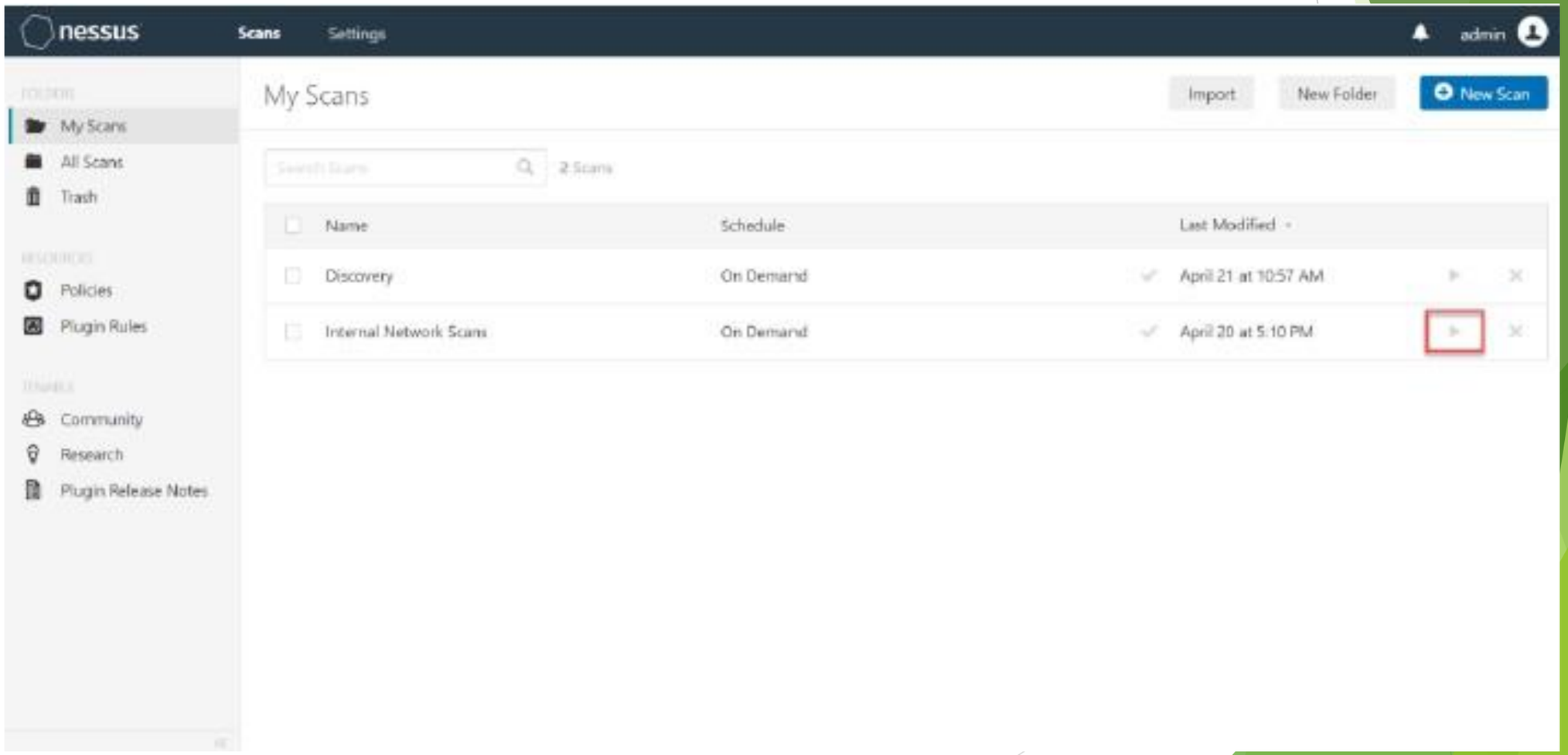
Create Scan

ทำการใส่ **Credentials** ของเครื่องปลายทางที่ต้องการสแกน



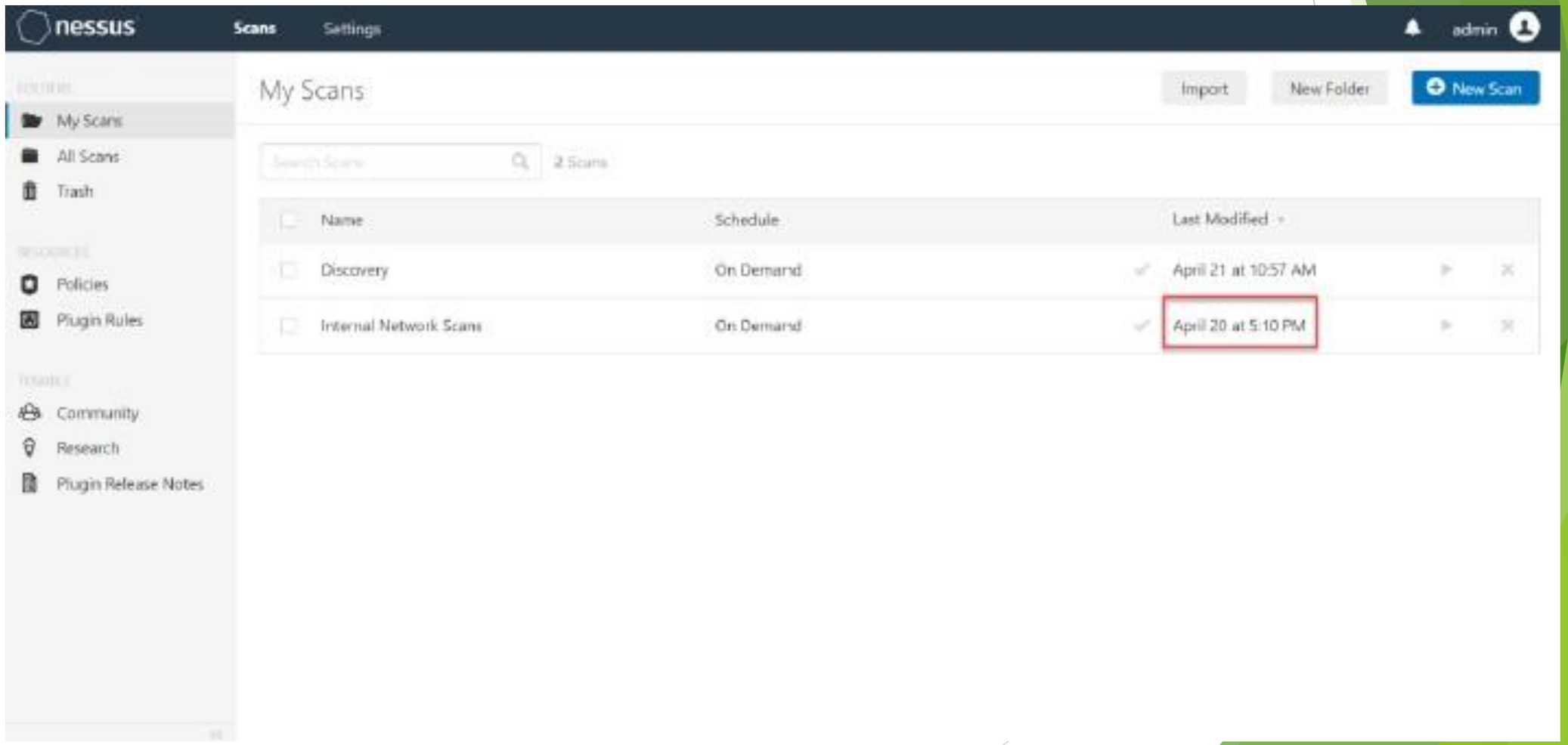
Create Scan

เมื่อทำการใส่ **Credentials** เสร็จทำการกดปุ่ม **Save** จากนั้นทำการกดที่ปุ่มสามเหลี่ยมในกรอบสีแดง เพื่อทำการสั่งสแกน



Create Scan

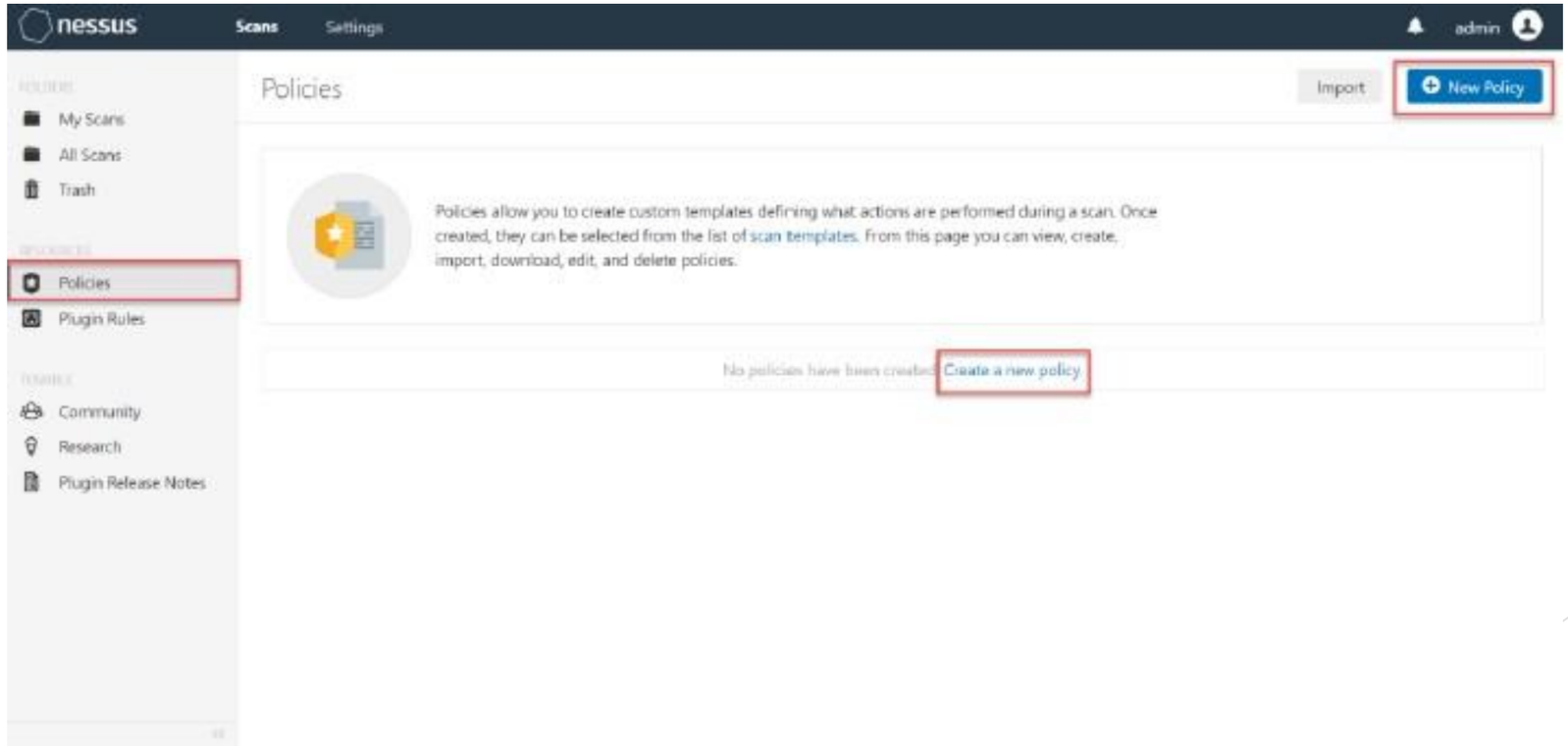
เมื่อทำการสแกนเสร็จ จะปรากฏข้อมูลตามภาพ ที่ทำการสแกนล่าสุด เป็นอันเสร็จ



Policies

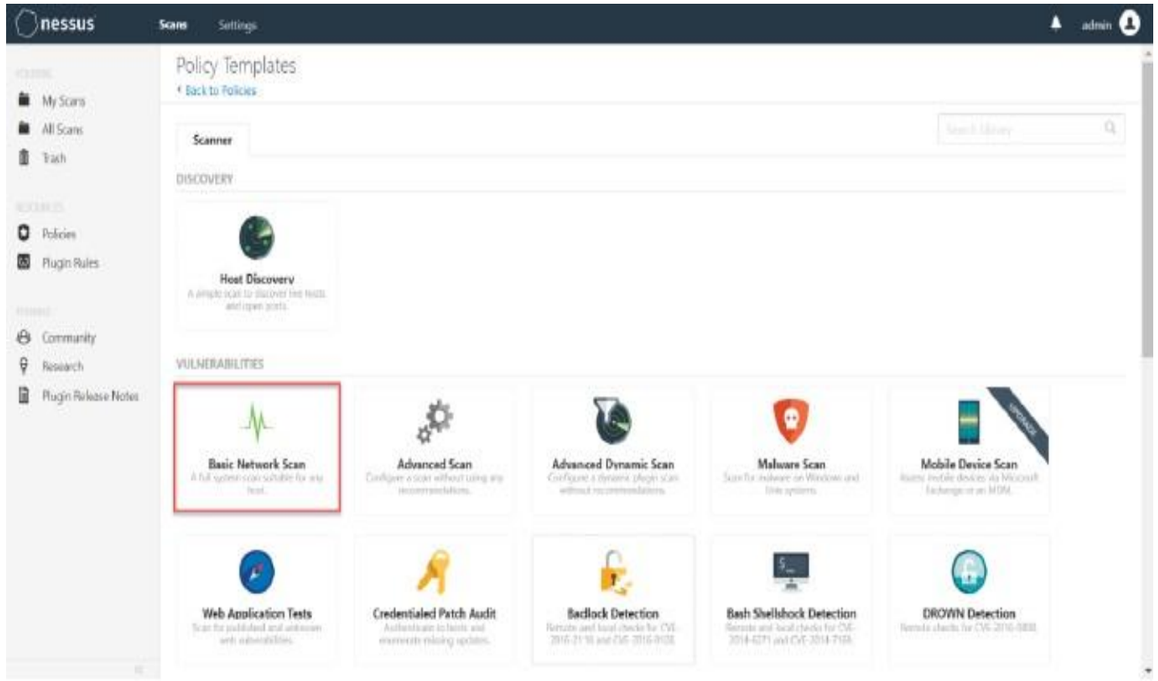
ในเมนูนี้สามารถสร้าง **Policy** ที่ใช้สำหรับการสแกนได้ ข้อดีคือสามารถใส่ตัว **Credentials** เป็น **Template** ไว้ได้ โดยไม่จำเป็นต้องใส่ **Credentials** ทุกครั้งที่สแกนใหม่

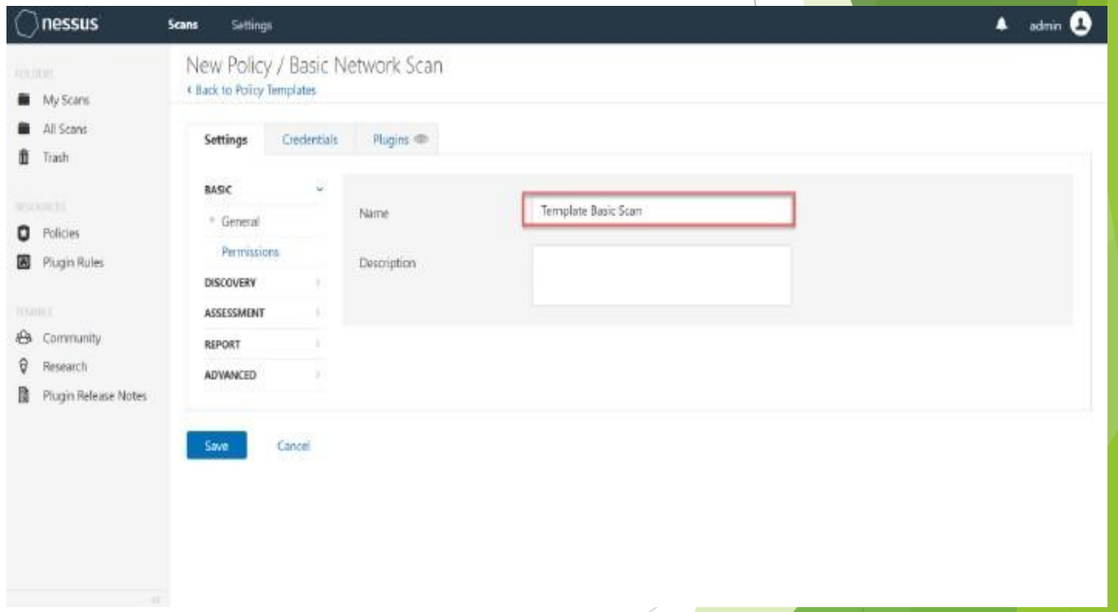
โดยไปที่เมนู **Policies** ในกรอบสีแดง จากนั้นกดที่ปุ่ม **New Policy** ที่มุมขวาบน หรือ **Create a new policy**



Policies

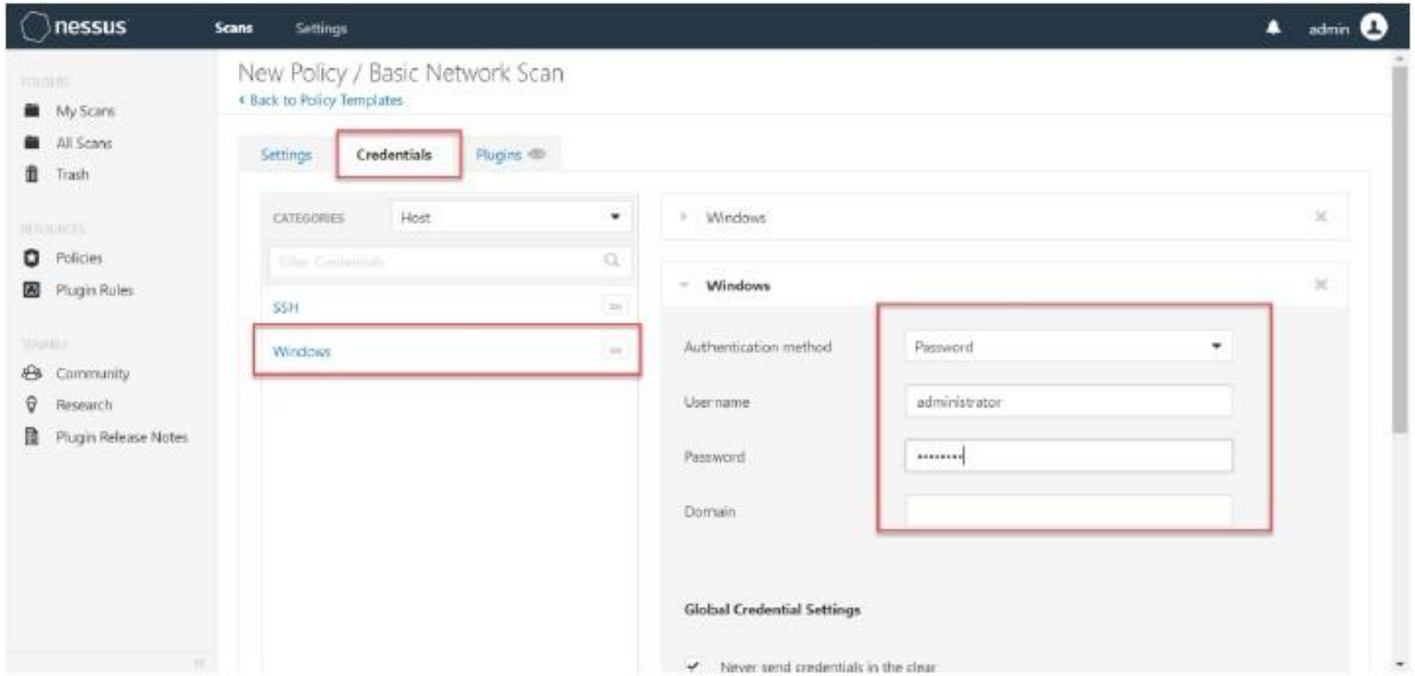
เลือก **Policy Scan** ที่ต้องการ เช่น **Basic Network Scan** แล้วใส่ชื่อ **Template Policy**





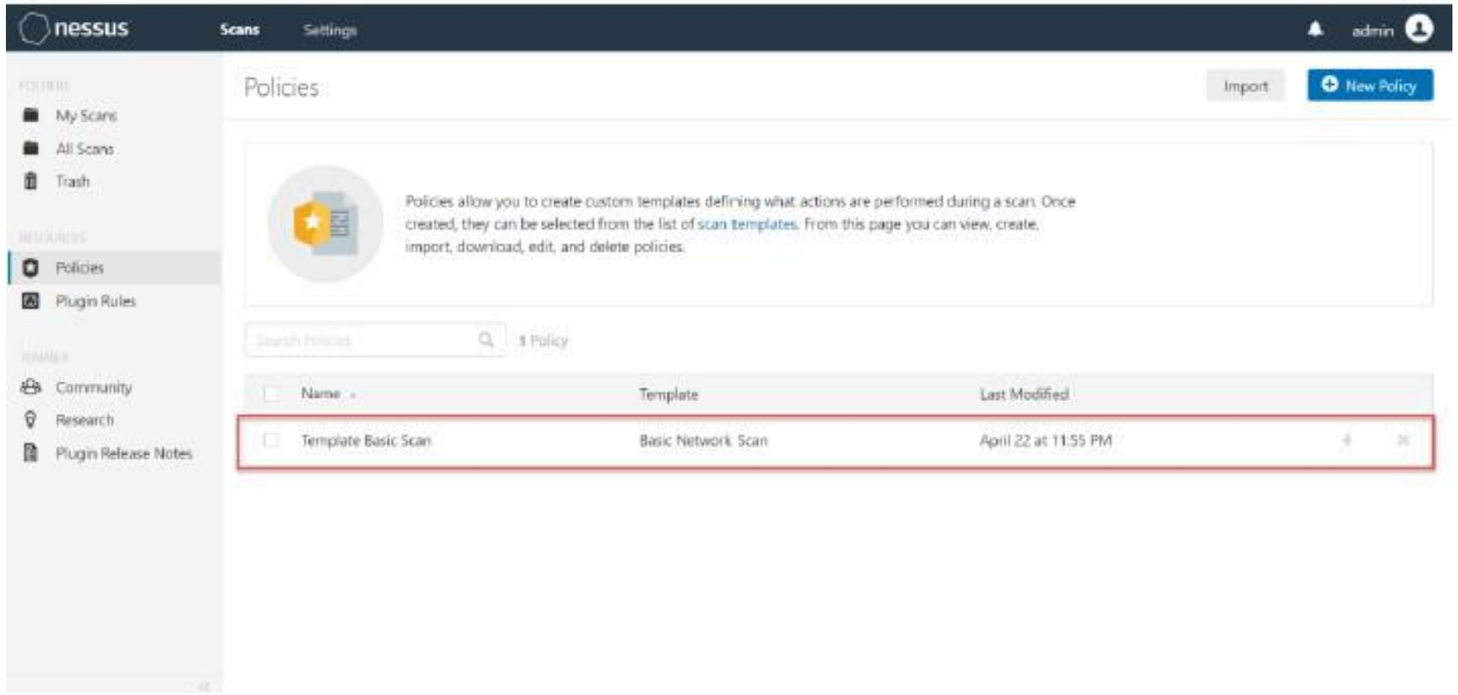
Policies

จากนั้นทำการใส่ **Credentials** สำหรับ **Template Policy** นี้ แล้วทำการกดปุ่ม **Save** เป็นอันเสร็จ



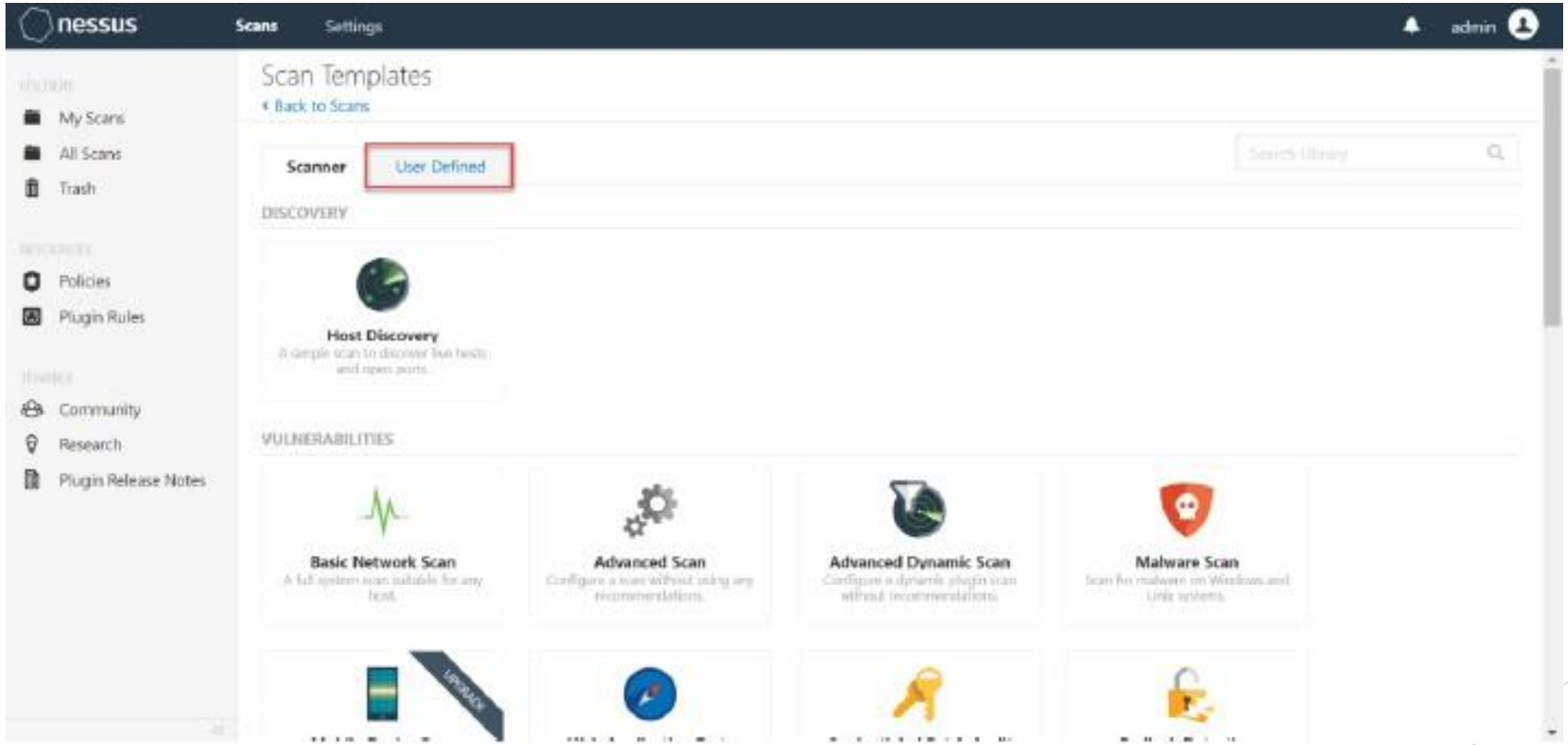
Policies

Template Policy ที่สร้างจะปรากฏขึ้นมา



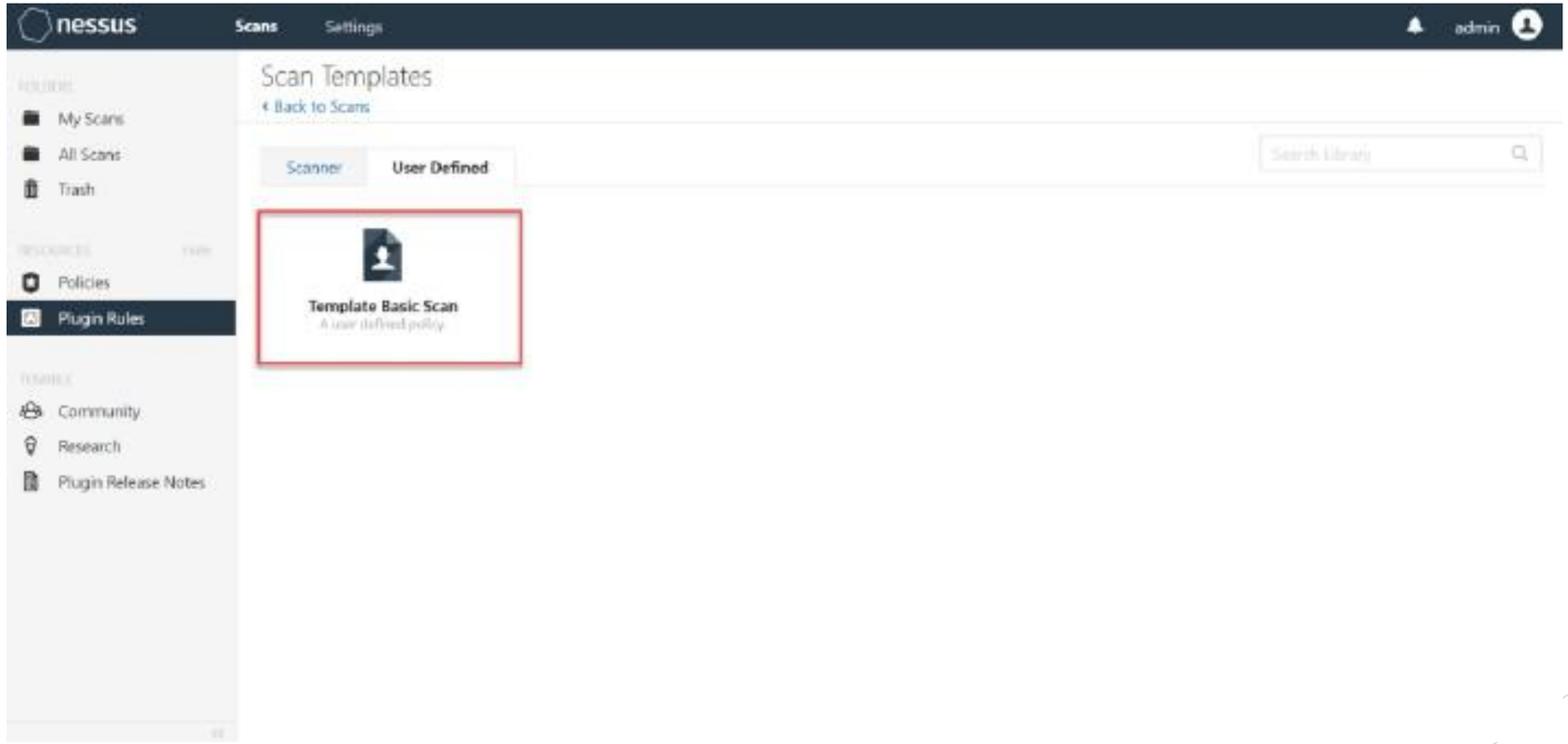
Policies

หากต้องการสแกนโดยใช้ **Template** ที่สร้างไว้ ให้ไปที่ **New Scan** เลือกหัวข้อ **User Defined**



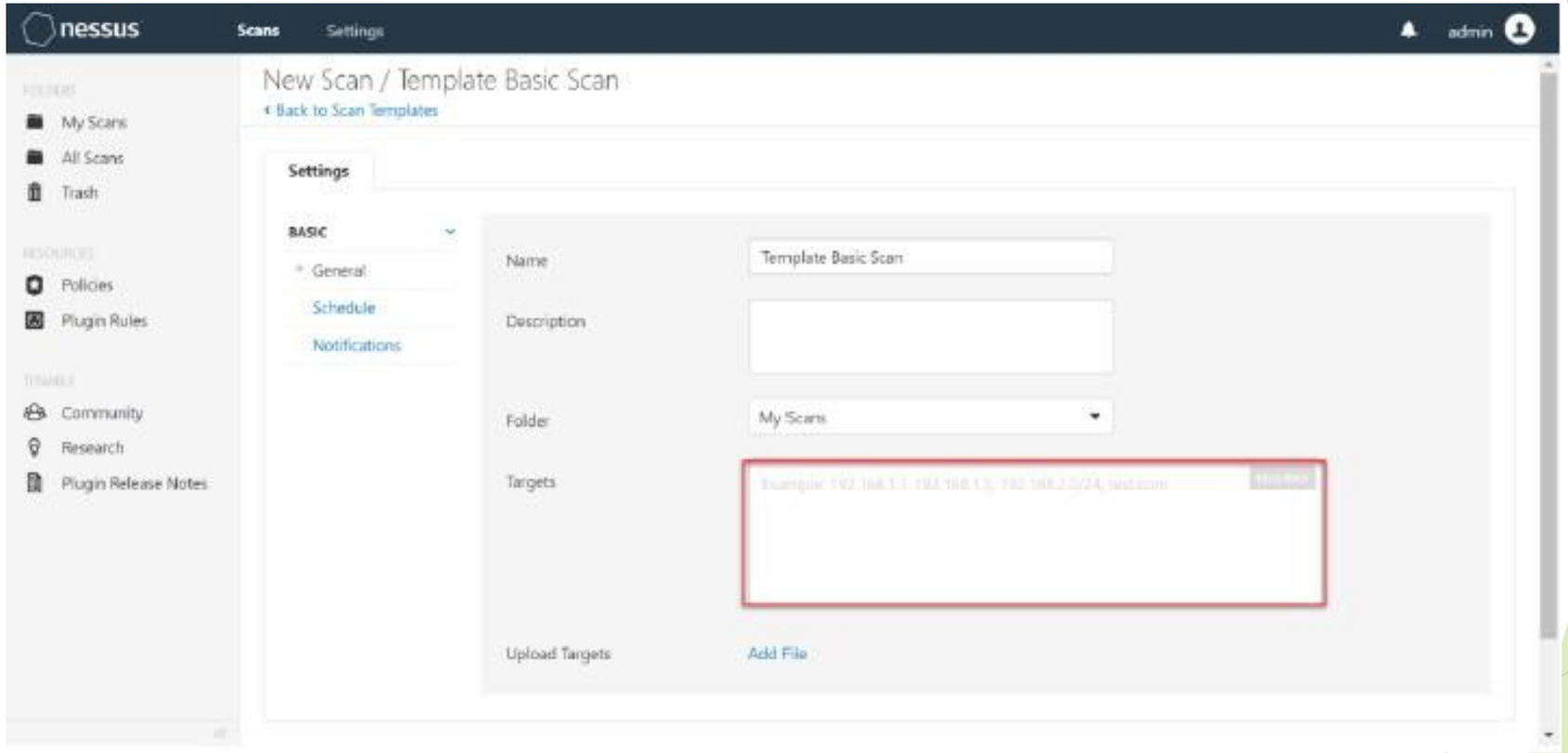
Policies

เลือก **Template** ที่เราสร้างไว้



Policies

ทำการใส่ **IP** หรือตั้งค่า **Schedule** กับ **Notifications** จากนั้นทำการกดปุ่ม Save เป็นอันเสร็จ



การแปลผลและรายงานการตรวจสอบ

แสดงรายละเอียดของช่องโหว่

โปรแกรม Nexes จะแสดงรายละเอียดของช่องโหว่ที่พบ รวมถึงระดับความรุนแรงและผลกระทบ ซึ่งจะช่วยให้ผู้ดูแลระบบสามารถวิเคราะห์และจัดลำดับความสำคัญของการแก้ไข

จัดทำรายงานการตรวจสอบ

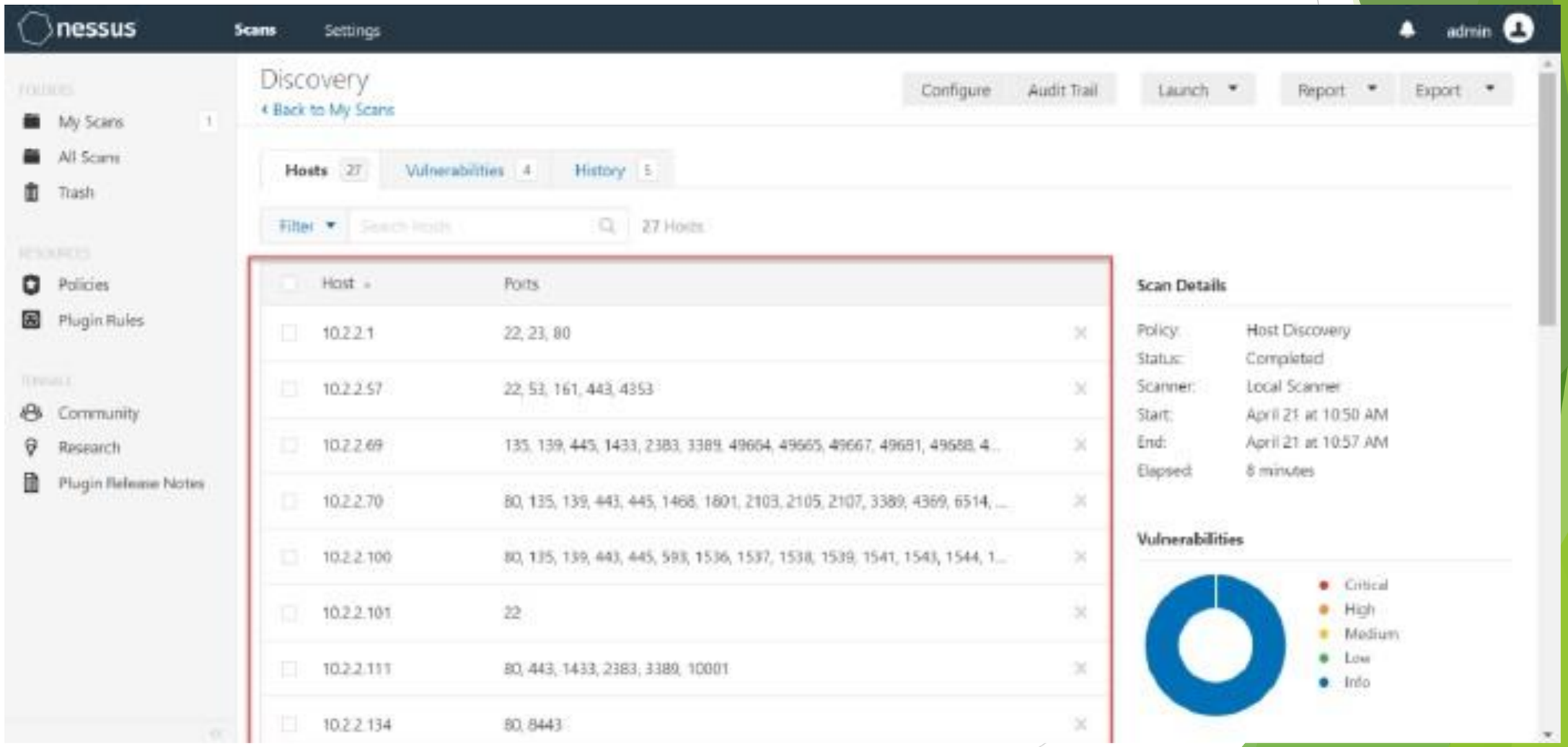
จัดทำรายงานการตรวจสอบแบบละเอียด ครอบคลุมข้อมูลเกี่ยวกับช่องโหว่ที่พบ ผลกระทบ และแนวทางการแก้ไข เพื่อนำเสนอต่อผู้บริหาร

ประสานงานและดำเนินการแก้ไข

ประสานงานกับทีมงานเทคนิคเพื่อวางแผนและดำเนินการปิดช่องโหว่อย่างเป็นขั้นตอน เพื่อเพิ่มระดับความปลอดภัยระบบไอทีโดยรวม

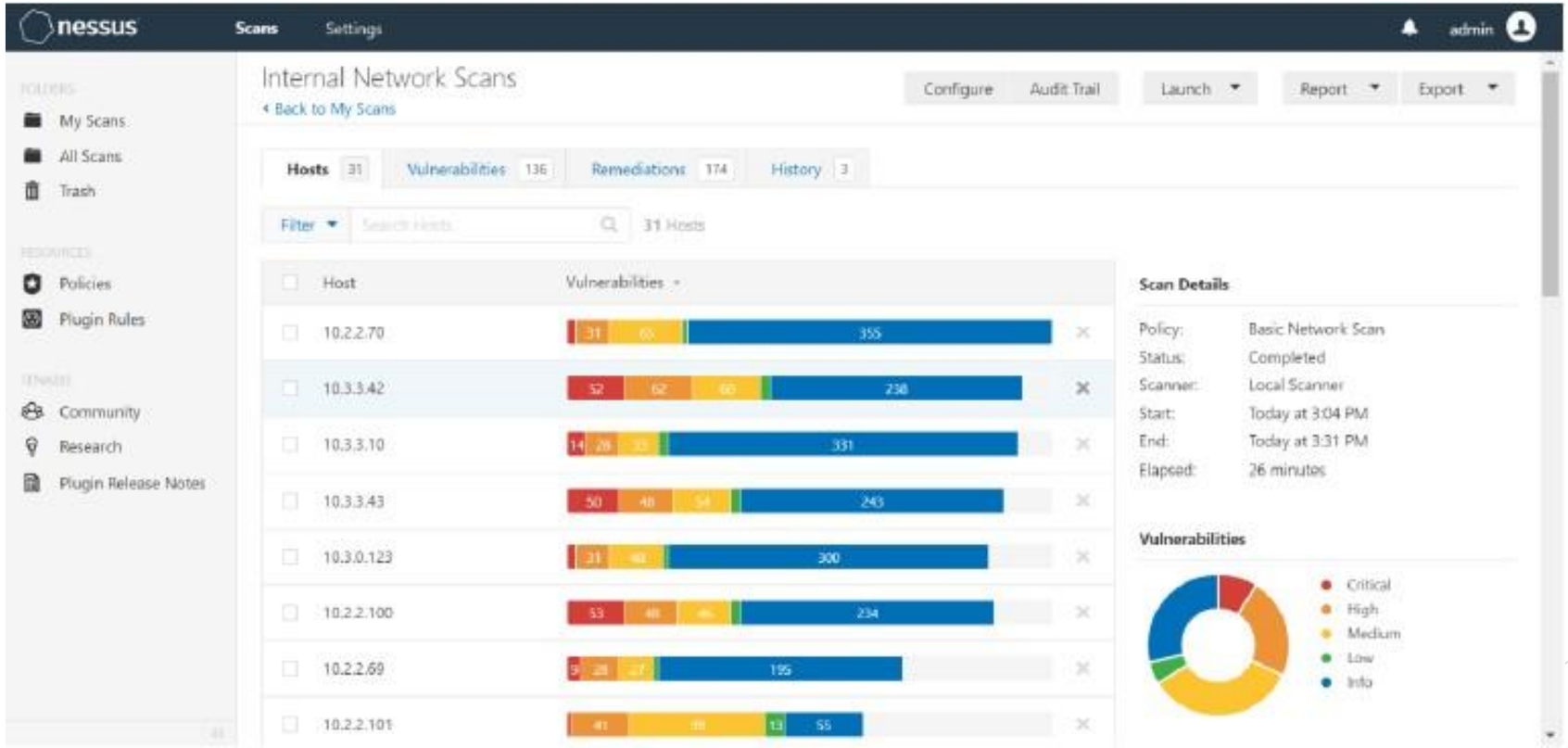
Scan Result

ผลลัพธ์ของการสแกนแบบ **Host Discovery** จะบอกเครื่องและ Port ที่เจอของเครื่องนั้นๆ



Scan Result

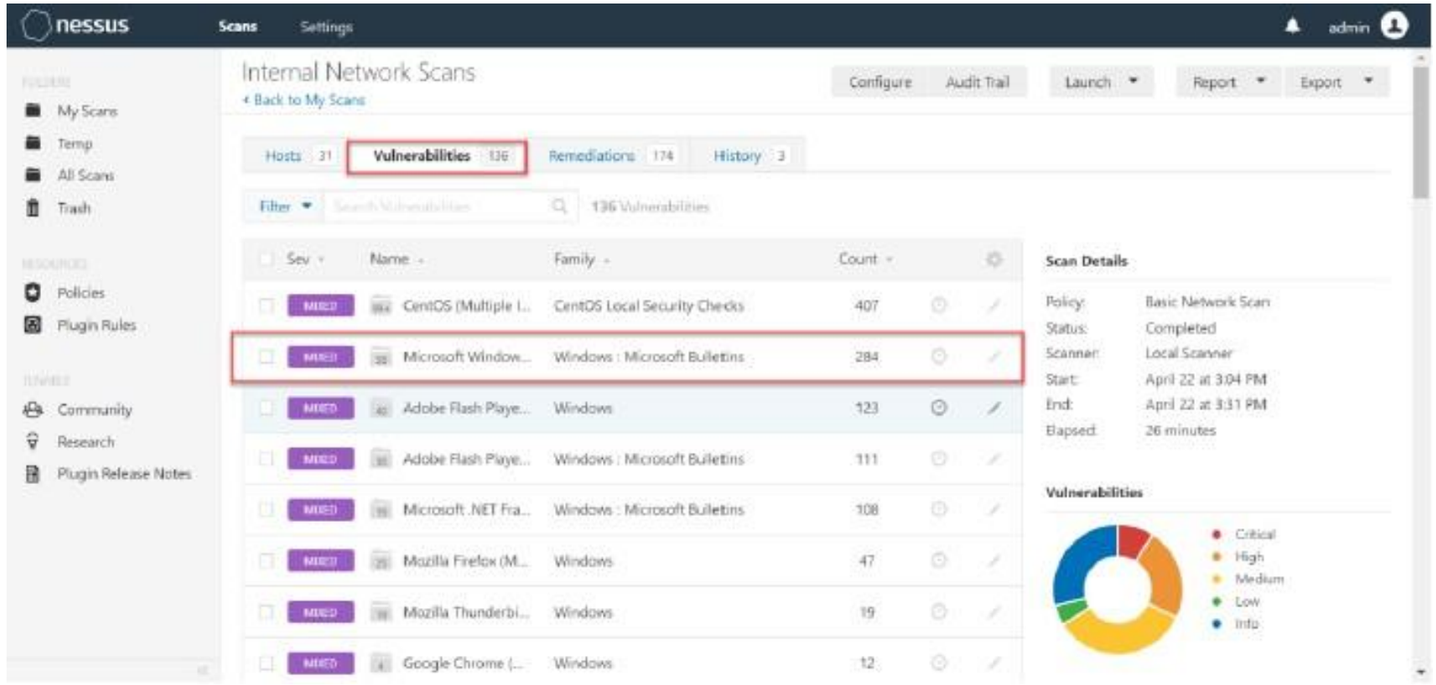
ผลลัพธ์ของการสแกนแบบ **Basic Network Scan** จะแสดงข้อมูลช่องโหว่ (Vulnerabilities) ระดับต่างๆที่เจอ



Troubleshooting

หลังจากทำการสแกนเสร็จ เราสามารถกดไปเข้าไปดูวิธีแก้ไขช่องโหว่ต่างๆได้

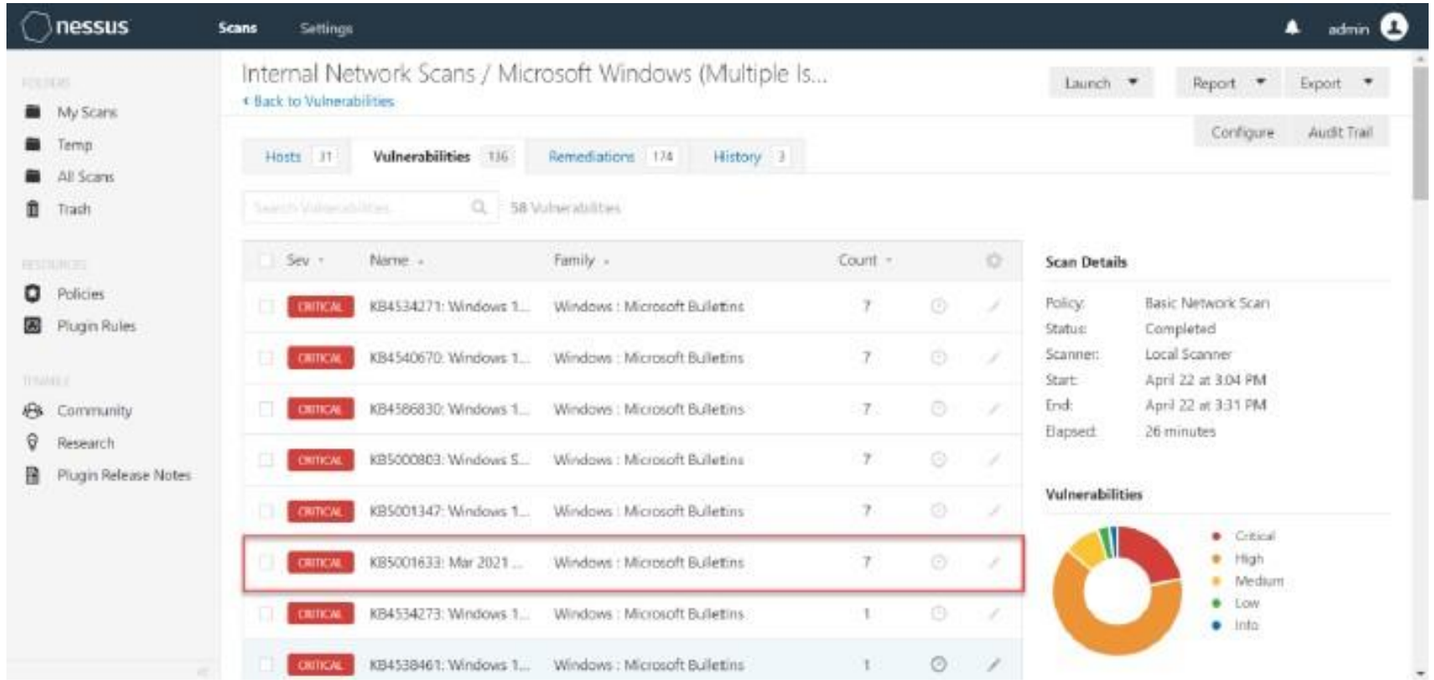
โดยทำการเลือก **Policy Scan** ที่ต้องการจะแก้ไขปัญหา > ไปที่เมนู **Vulnerabilities** แล้วเลือกช่องโหว่ที่ต้องการ



Troubleshooting

เมื่อกดเข้ามา ก็จะเห็นรายละเอียด ของ **Family Windows** ตัวนี้ว่ามีช่องโหว่หรือ **Plugin** อะไรบ้างที่เกี่ยวข้อง

ให้ทำการเลือกช่องโหว่ที่ต้องการแก้ไข



Troubleshooting

ข้อมูลต่างๆเกี่ยวกับ **Plugin** ตัวนี้จะปรากฏขึ้นมาดังนี้

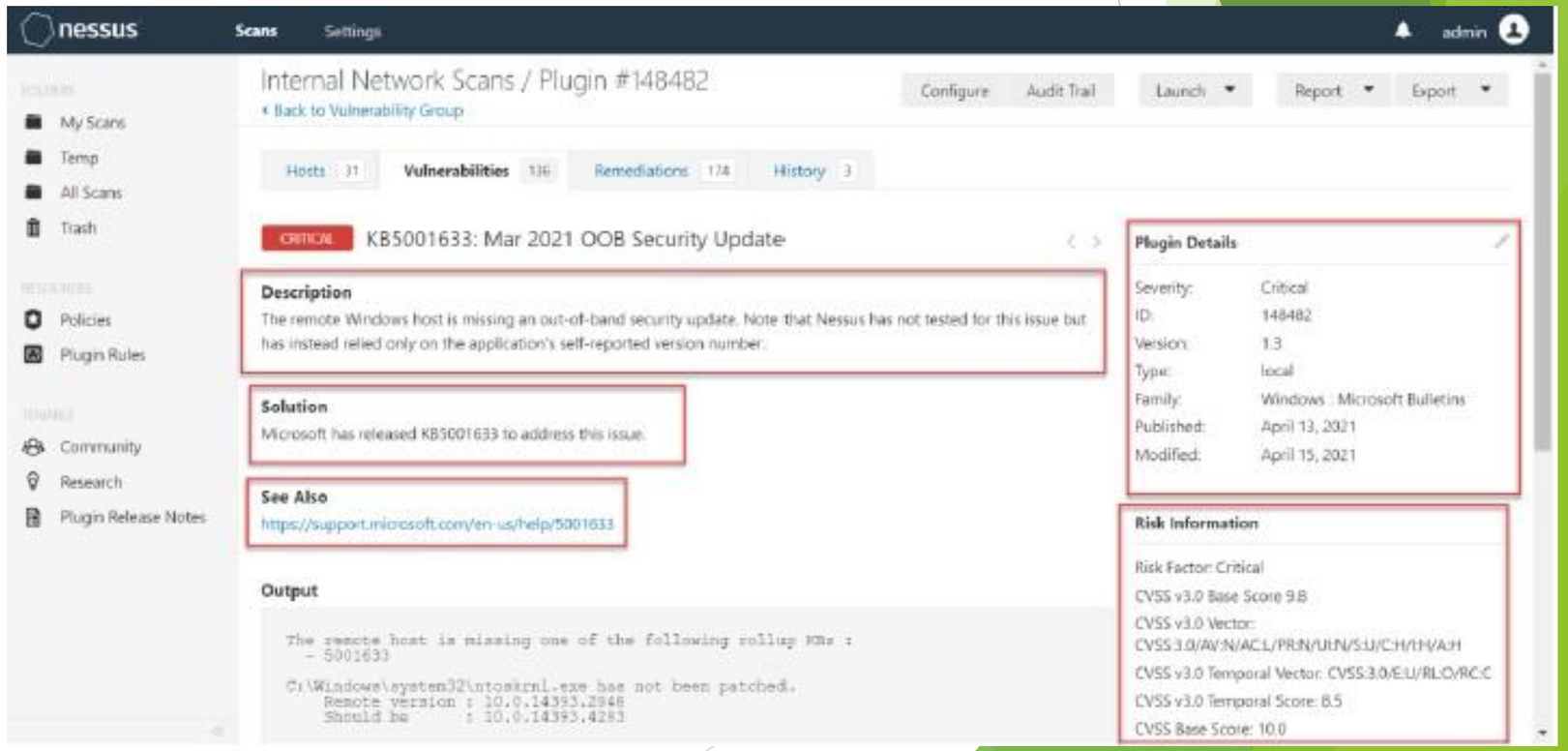
Description : จะบอกรายละเอียดเกี่ยวกับช่องโหว่ตัวนี้

Solution : วิธีแก้ไขช่องโหว่ตัวนี้

See Also : รายละเอียดเพิ่มเติมเกี่ยวกับช่องโหว่ตัวนี้

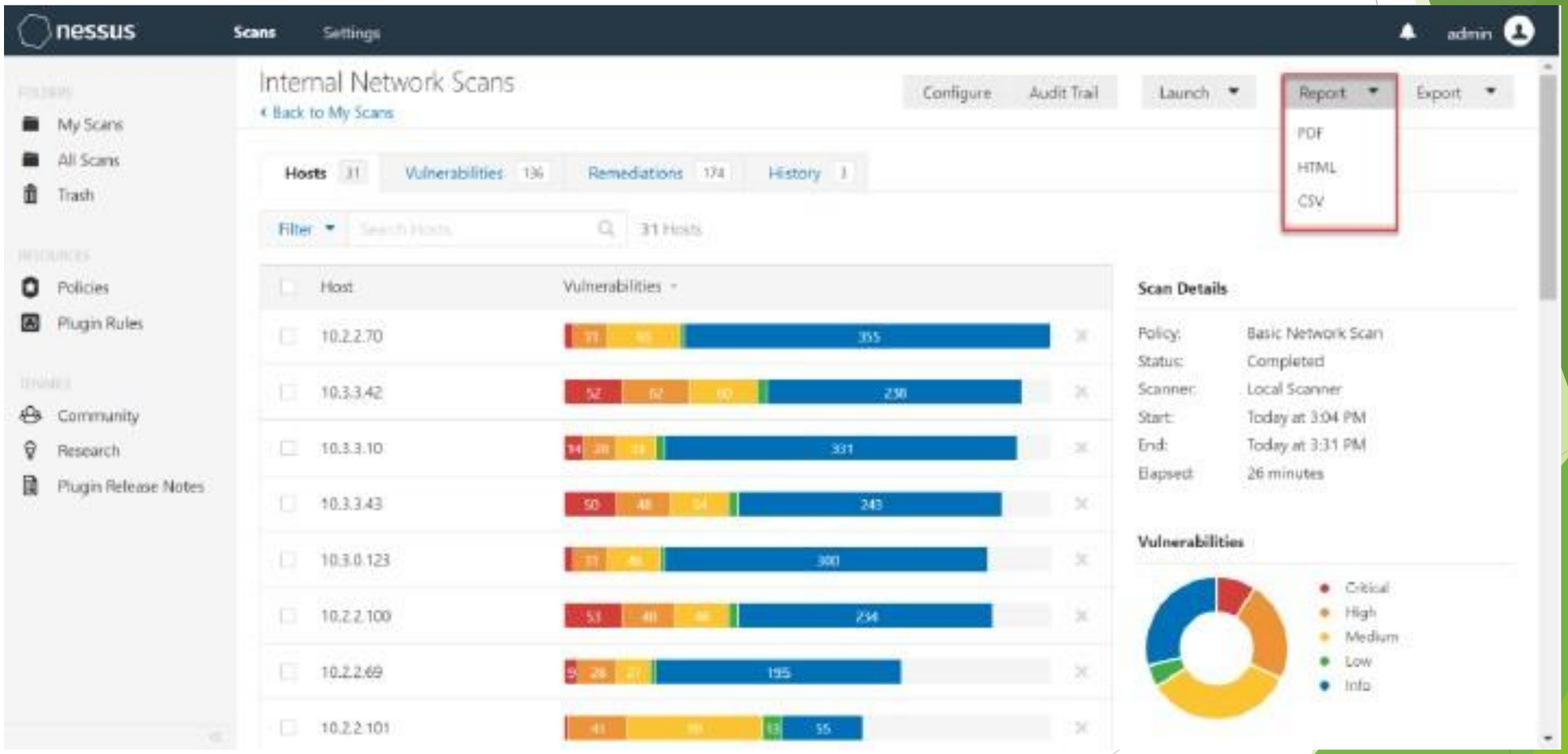
Plugin Details : ข้อมูลเกี่ยวกับช่องโหว่

Risk Information : ข้อมูล Score ของช่องโหว่ตัวนี้



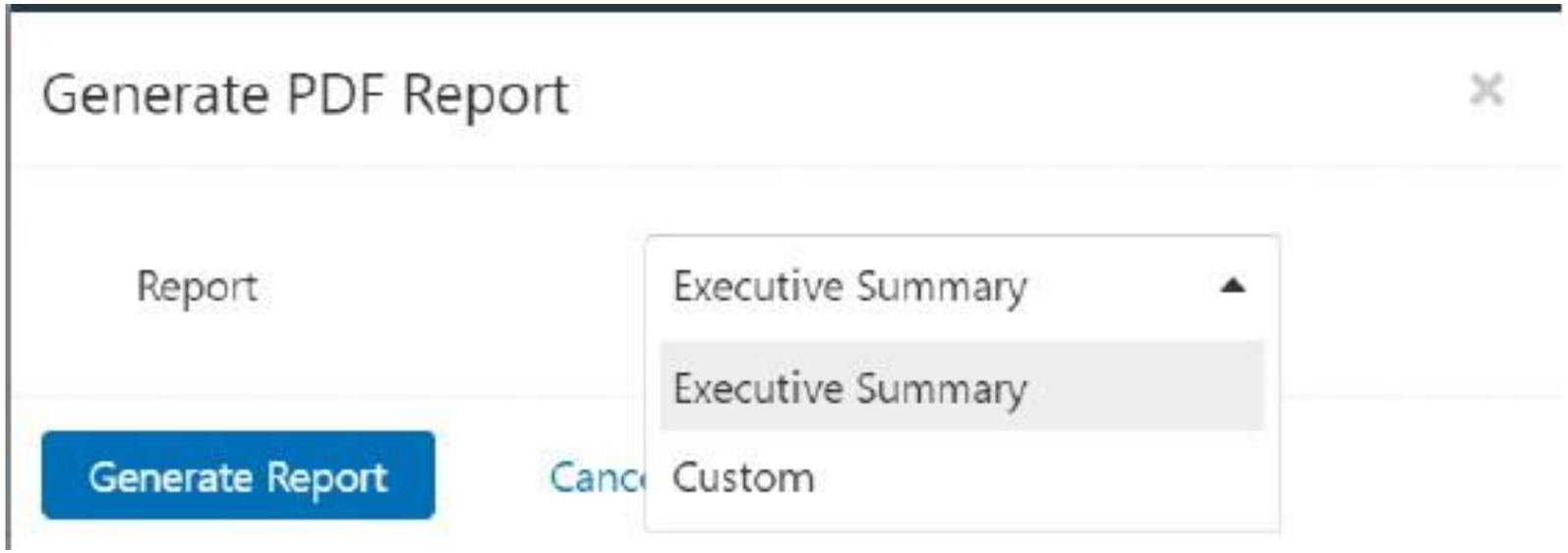
Report

ทำการเลือก **Policy Scan** และประเภทของ **Report (PDF , HTML , CSV)** ที่ต้องการ



Report

ประเภทข้อมูลของ **Report** จะมีให้เลือก **2** แบบคือ **Executive Summary** และ **Custom**



Report

ตัวอย่าง **Report** แบบ **Executive Summary**

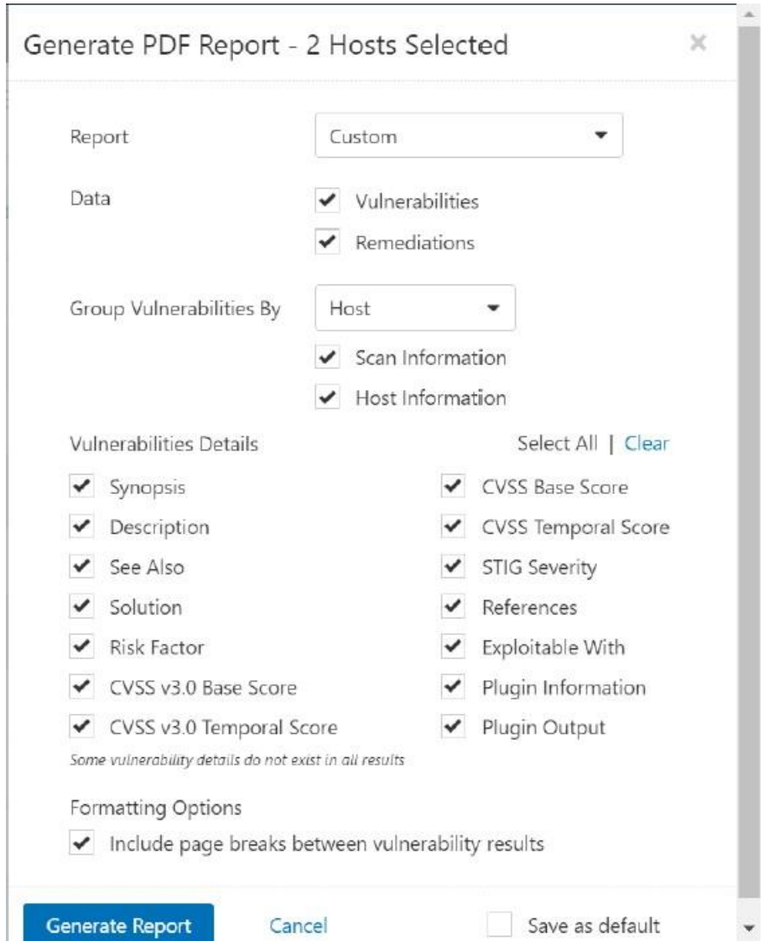
52	62	54	5	137
CRITICAL	HIGH	MEDIUM	LOW	INFO

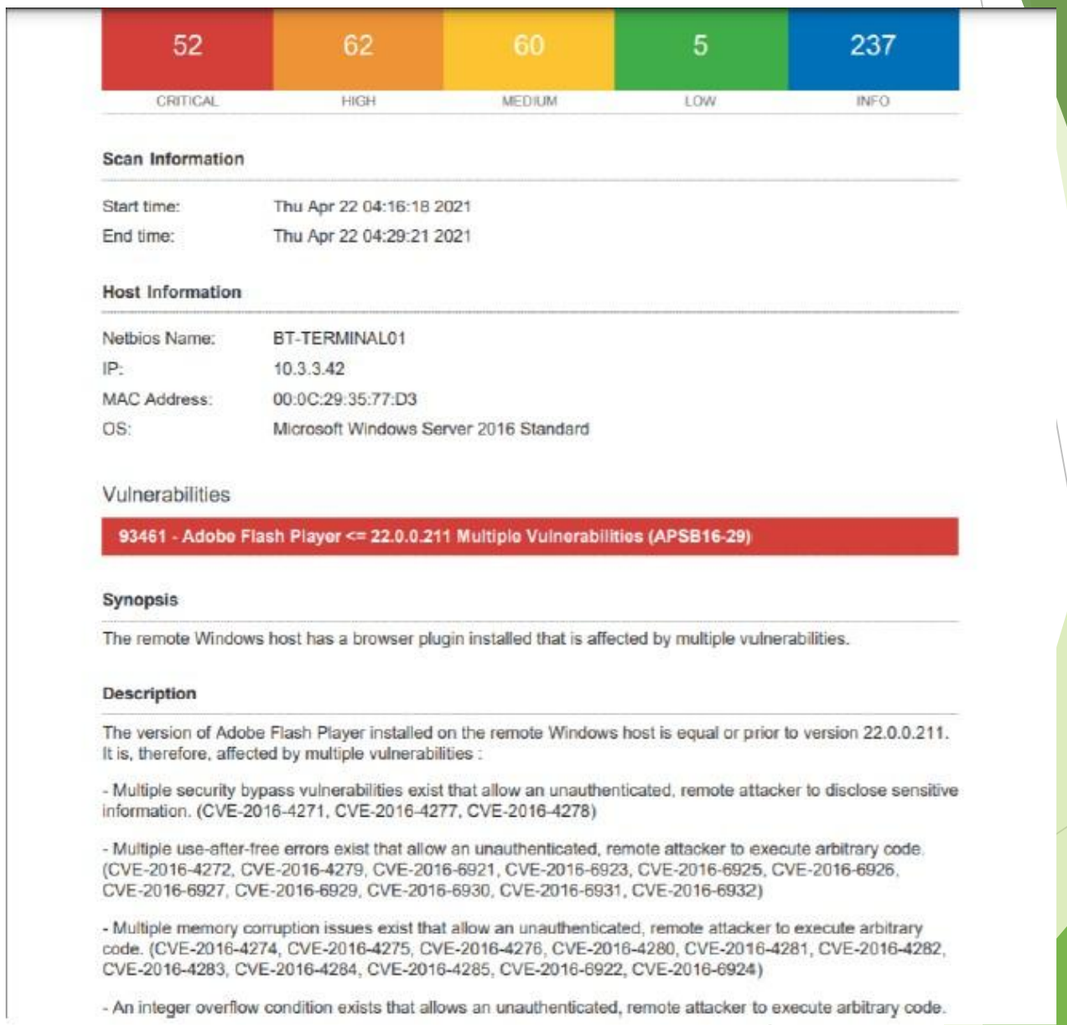
Vulnerabilities Total: 310

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	93461	Adobe Flash Player <= 22.0.0.211 Multiple Vulnerabilities (APSB16-29)
CRITICAL	10.0	93960	Adobe Flash Player <= 23.0.0.162 Multiple Vulnerabilities (APSB16-32)
CRITICAL	10.0	95762	Adobe Flash Player <= 23.0.0.207 Multiple Vulnerabilities (APSB16-39)
CRITICAL	10.0	96388	Adobe Flash Player <= 24.0.0.186 Multiple Vulnerabilities (APSB17-02)
CRITICAL	10.0	97142	Adobe Flash Player <= 24.0.0.194 Multiple Vulnerabilities (APSB17-04)
CRITICAL	10.0	97727	Adobe Flash Player <= 24.0.0.221 Multiple Vulnerabilities (APSB17-07)
CRITICAL	10.0	99283	Adobe Flash Player <= 25.0.0.127 Multiple Vulnerabilities (APSB17-10)
CRITICAL	10.0	100052	Adobe Flash Player <= 25.0.0.148 Multiple Vulnerabilities (APSB17-15)
CRITICAL	10.0	100756	Adobe Flash Player <= 25.0.0.171 Multiple Vulnerabilities (APSB17-17)
CRITICAL	10.0	101362	Adobe Flash Player <= 26.0.0.131 Multiple Vulnerabilities (APSB17-21)
CRITICAL	10.0	104544	Adobe Flash Player <= 27.0.0.183 (APSB17-33)

Report

ตัวอย่าง **Report** แบบ **Custom**





52	62	60	5	237
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Thu Apr 22 04:16:18 2021
End time: Thu Apr 22 04:29:21 2021

Host Information

Netbios Name: BT-TERMINAL01
IP: 10.3.3.42
MAC Address: 00:0C:29:35:77:D3
OS: Microsoft Windows Server 2016 Standard

Vulnerabilities

93461 - Adobe Flash Player <= 22.0.0.211 Multiple Vulnerabilities (APSB16-29)

Synopsis

The remote Windows host has a browser plugin installed that is affected by multiple vulnerabilities.

Description

The version of Adobe Flash Player installed on the remote Windows host is equal or prior to version 22.0.0.211. It is, therefore, affected by multiple vulnerabilities :

- Multiple security bypass vulnerabilities exist that allow an unauthenticated, remote attacker to disclose sensitive information. (CVE-2016-4271, CVE-2016-4277, CVE-2016-4278)

- Multiple use-after-free errors exist that allow an unauthenticated, remote attacker to execute arbitrary code. (CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, CVE-2016-6932)

- Multiple memory corruption issues exist that allow an unauthenticated, remote attacker to execute arbitrary code. (CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, CVE-2016-6924)

- An integer overflow condition exists that allows an unauthenticated, remote attacker to execute arbitrary code.

ตัวอย่างรายงาน

CRITICAL **Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF**

Description

The version of Apache httpd installed on the remote host is equal to or greater than 2.4.7 and prior to 2.4.52. It is, therefore, affected by a flaw related to acting as a forward proxy.

A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.52 or later.

Output

```
URL               : http://dohmeeting.anamai.moph.go.th/
Installed version : 2.4.38
Fixed version     : 2.4.52
```

Plugin Details

Severity:	Critical
ID:	156255
Version:	1.10
Type:	combined
Family:	Web Servers
Published:	December 23, 2021
Modified:	November 22, 2023

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: PoC
Age of Vuln: 730 days +
Product Coverage: Very High
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

ตัวอย่างรายงาน

CRITICAL PHP 7.4.x < 7.4.28

Description

The version of PHP installed on the remote host is prior to 7.4.28. It is, therefore, affected by a vulnerability as referenced in the Version 7.4.28 advisory.

- In PHP versions 7.4.x below 7.4.28, 8.0.x below 8.0.16, and 8.1.x below 8.1.3, when using filter functions with FILTER_VALIDATE_FLOAT filter and min/max limits, if the filter fails, there is a possibility to trigger use of allocated memory after free, which can result it crashes, and potentially in overwrite of other memory chunks and RCE. This issue affects: code that uses FILTER_VALIDATE_FLOAT with min/max limits.
(CVE-2021-21708)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to PHP version 7.4.28 or later.

See Also

http://php.net/ChangeLog-7.php#7.4.28

Plugin Details

Severity:	Critical
ID:	158133
Version:	1.8
Type:	remote
Family:	CGI abuses
Published:	February 17, 2022
Modified:	November 22, 2024

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: PoC
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

ตัวอย่างรายงาน

CRITICAL OpenSSL 3.1.0 < 3.1.7 Vulnerability

Description

The version of OpenSSL installed on the remote host is prior to 3.1.7. It is, therefore, affected by a vulnerability as referenced in the 3.1.7 advisory.

- Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash.
In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a no overlap response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to

Plugin Details

Severity:	Critical
ID:	201082
Version:	1.3
Type:	combined
Family:	Web Servers
Published:	June 27, 2024
Modified:	October 7, 2024

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 180 - 365 days
Product Coverage: Low
CVSSV3 Impact Score: 5.2
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 6.0
Exploit Prediction Scoring System (EPSS): 0.0004
Risk Factor: Medium
CVSS v3.0 Base Score: 9.1

แนวทางการแก้ไขช่องโหว่และเพิ่มระดับความปลอดภัย

1 **ปรับปรุงการตั้งค่าระบบ**

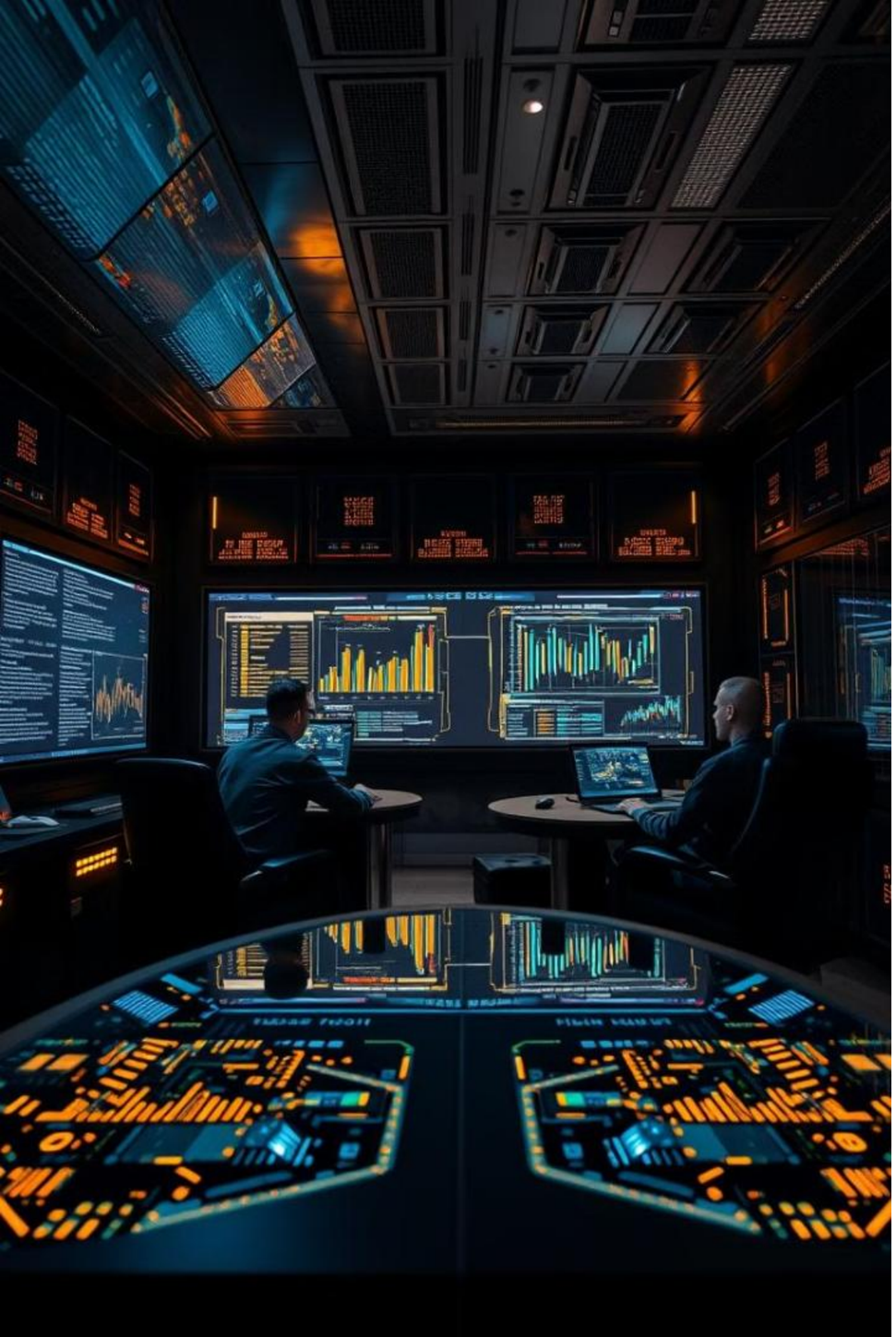
อัพเดทซอฟต์แวร์, เปลี่ยนรหัสผ่าน และ จำกัดการเข้าถึงข้อมูล

2 **ติดตั้งระบบและเครื่องมือรักษาความปลอดภัย**

Firewall,ระบบตรวจจับการบุกรุก (IPS) หรือ ซอฟต์แวร์ป้องกันไวรัส(Anti-Virus)

3 **จัดทำแผนรับมือและซ้อมแผนรับมือ**

เพื่อทันต่อเหตุการณ์ที่อาจเกิดขึ้นทางไซเบอร์อย่างต่อเนื่อง



สรุปและแนะนำแนวทางปฏิบัติ

ช่วยตรวจพบจุดอ่อน

การใช้โปรแกรม Nexes ช่วยให้สามารถตรวจพบจุดอ่อนในระบบไอทีเบื้องต้นได้อย่างมีประสิทธิภาพ และเป็นจุดเริ่มต้นในการยกระดับความปลอดภัยทางไซเบอร์อย่างเป็นระบบ

ปิดช่องโหว่อย่างต่อเนื่อง

แนะนำให้องค์กรสำรวจและ ปิดช่องโหว่ที่พบอย่างต่อเนื่อง ควบคู่กับการจัดทำนโยบายและแผนบริหารความเสี่ยงด้านไซเบอร์อย่างเป็นรูปธรรม

Thankyou

Q&A