

Vulnerability Assessment

Tenable Nessus

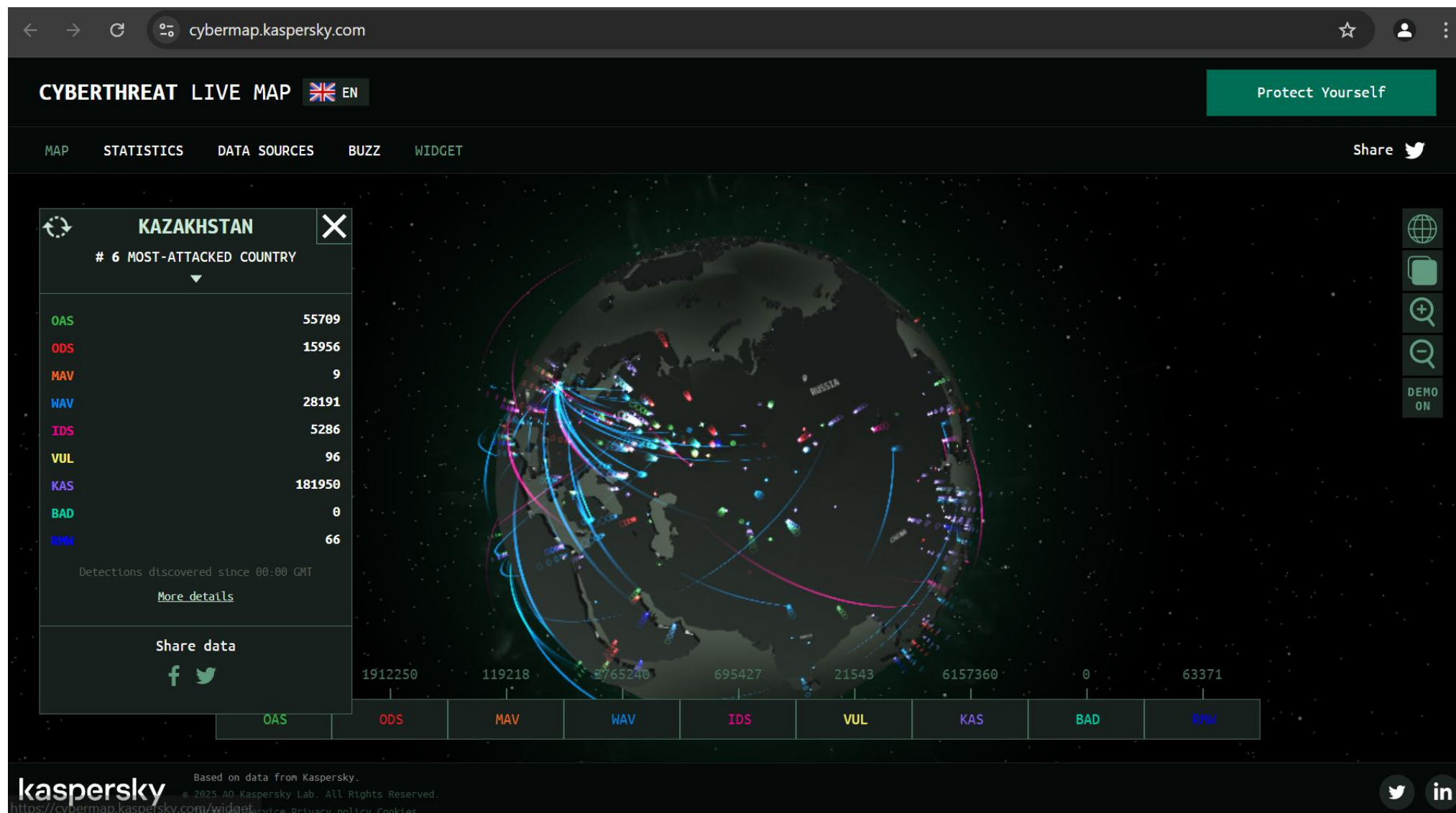
การวิเคราะห์และประเมินจุดอ่อน

ภัยคุกคามทางไซเบอร์



ภัยคุกคามทางไซเบอร์

► <https://cybermap.kaspersky.com/>



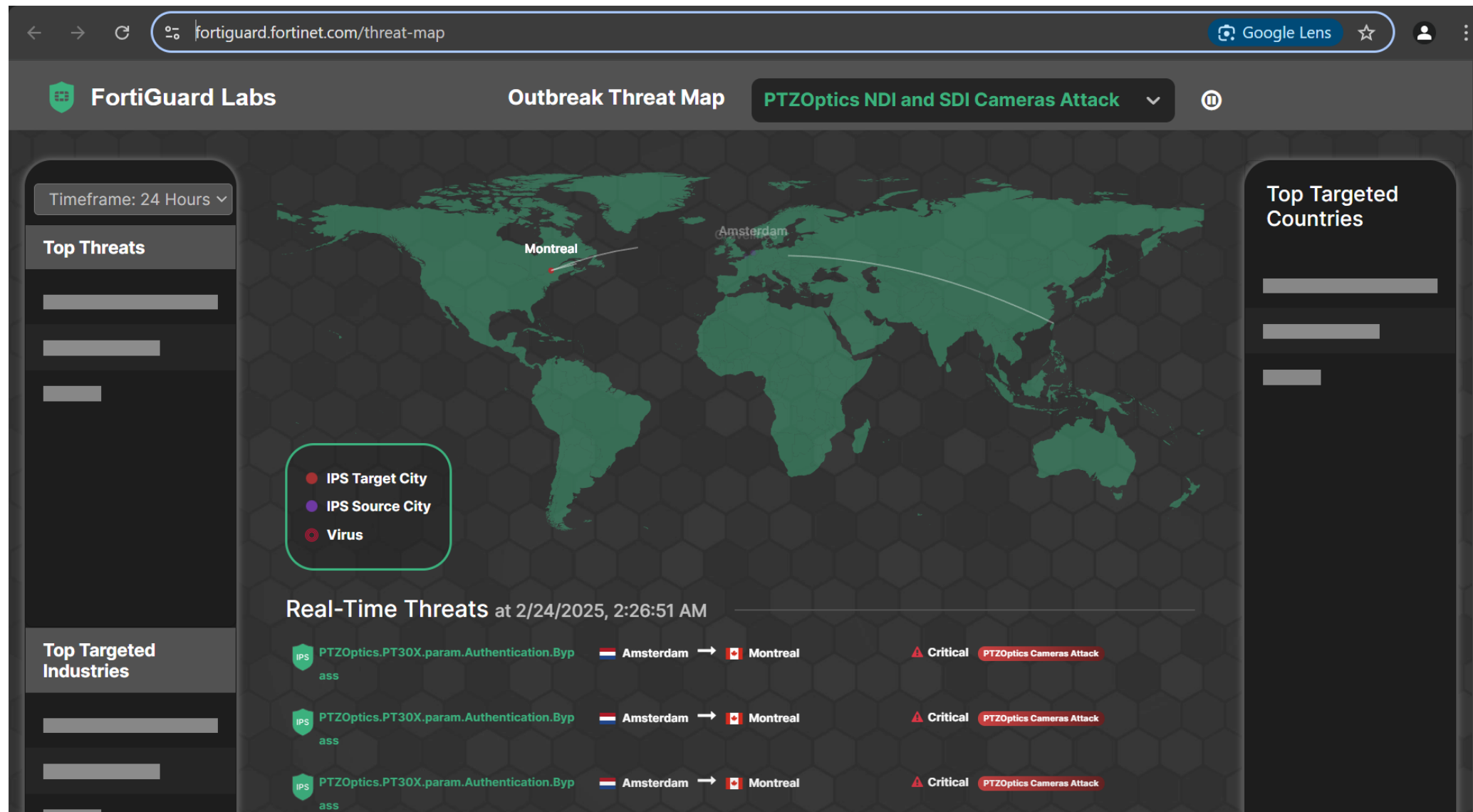
ภัยคุกคามทางไซเบอร์

► <https://livethreatmap.radware.com/>



ภัยคุกคามทางไซเบอร์

► <https://fortiguard.fortinet.com/threat-map>



Common Vulnerabilities and Exposures (CVE)

▶ <https://www.cvedetails.com/>

The screenshot shows the CVE Details website dashboard. The page features a navigation menu on the left with categories like Vulnerabilities, Vulnerable Software, and Vulnerability Intel. The main content area includes a search bar, a 'New/Updated CVEs' section with a donut chart and statistics, a 'Known exploited vulnerabilities' table, a 'Recent EPSS score changes' table, and a 'Distribution of vulnerabilities by CVSS scores' horizontal bar chart. A weighted average CVSS score of 7.6 is also displayed.

New/Updated CVEs

- 61 CVEs created, 94 CVEs updated since yesterday
- 632 CVEs created, 1894 CVEs updated in the last 7 days
- 3092 CVEs created, 9313 CVEs updated in the last 30 days

Known exploited vulnerabilities

Since yesterday	Last 7 days	Last 30 days
0	5	24

Recent EPSS score changes

>5%	>10%	>50%
19	5	1

Distribution of vulnerabilities by CVSS scores

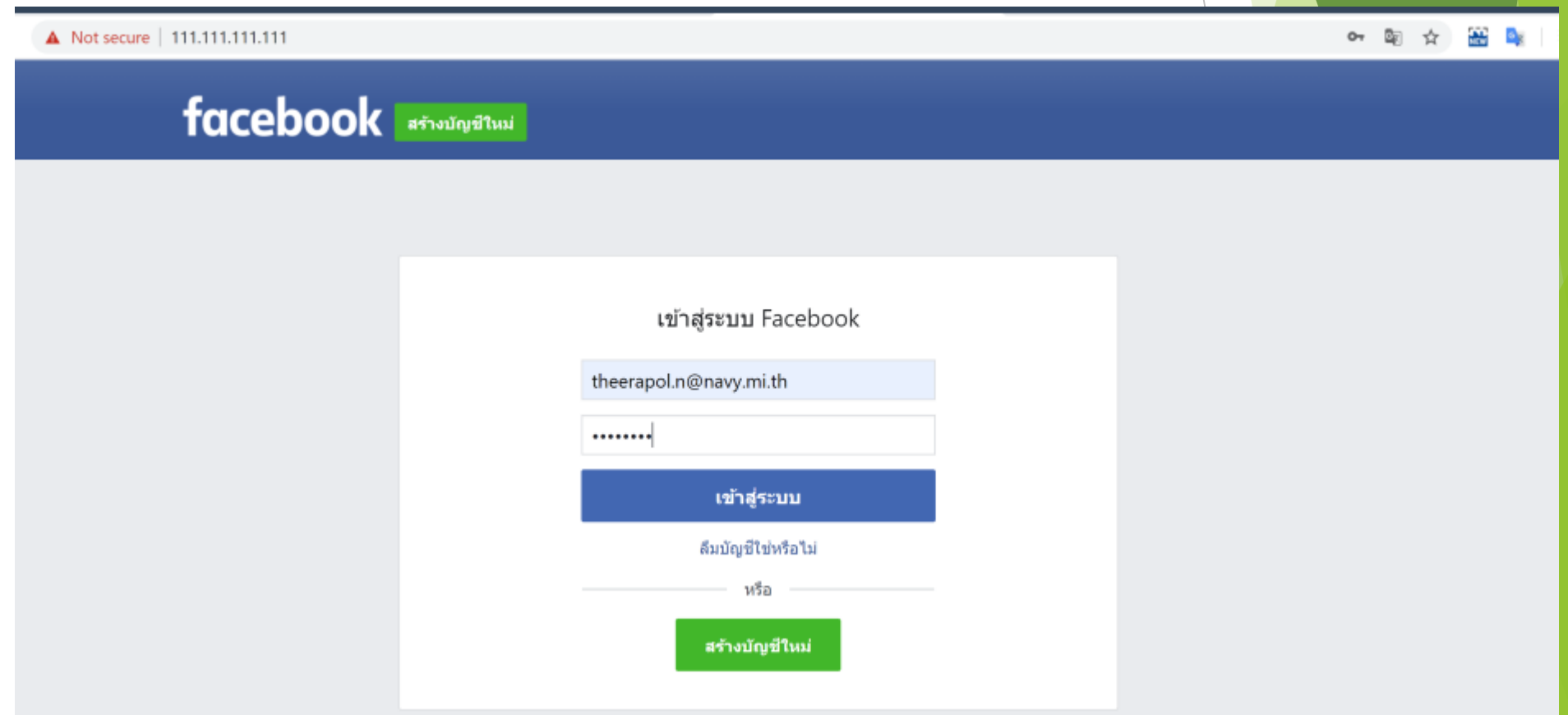
CVSS Score Range	Vulnerabilities
0-1	2241
1-2	96
2-3	865
3-4	2219
4-5	15054
5-6	33209
6-7	34328
7-8	51036
8-9	25496
9+	36377
Total	200921

Weighted Average CVSS Score: 7.6

* For CVEs published in the last 10 years

ภัยคุกคามทางไซเบอร์

- ▶ การหลอกลวงเพื่อเอาข้อมูล
- ▶ ขโมยข้อมูล
- ▶ เตาสุ่ม
- ▶ **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_Denv	A1:2017-Iniection	



ความสำคัญของการรักษาความมั่นคง ปลอดภัยทางไซเบอร์

ป้องกันการเข้าถึงข้อมูลและระบบของธุรกิจจากผู้ไม่ประสงค์ดี ซึ่งอาจส่งผลกระทบต่อ
กระทบร้ายแรงต่อการดำเนินงานและชื่อเสียง

สร้างความไว้วางใจและความมั่นใจให้กับลูกค้า พนักงาน และหุ้นส่วนของธุรกิจ
ในการรับมือความรับผิดชอบในการปกป้องข้อมูลที่สำคัญ

ความรู้เบื้องต้นเกี่ยวกับโปรแกรม Nessus

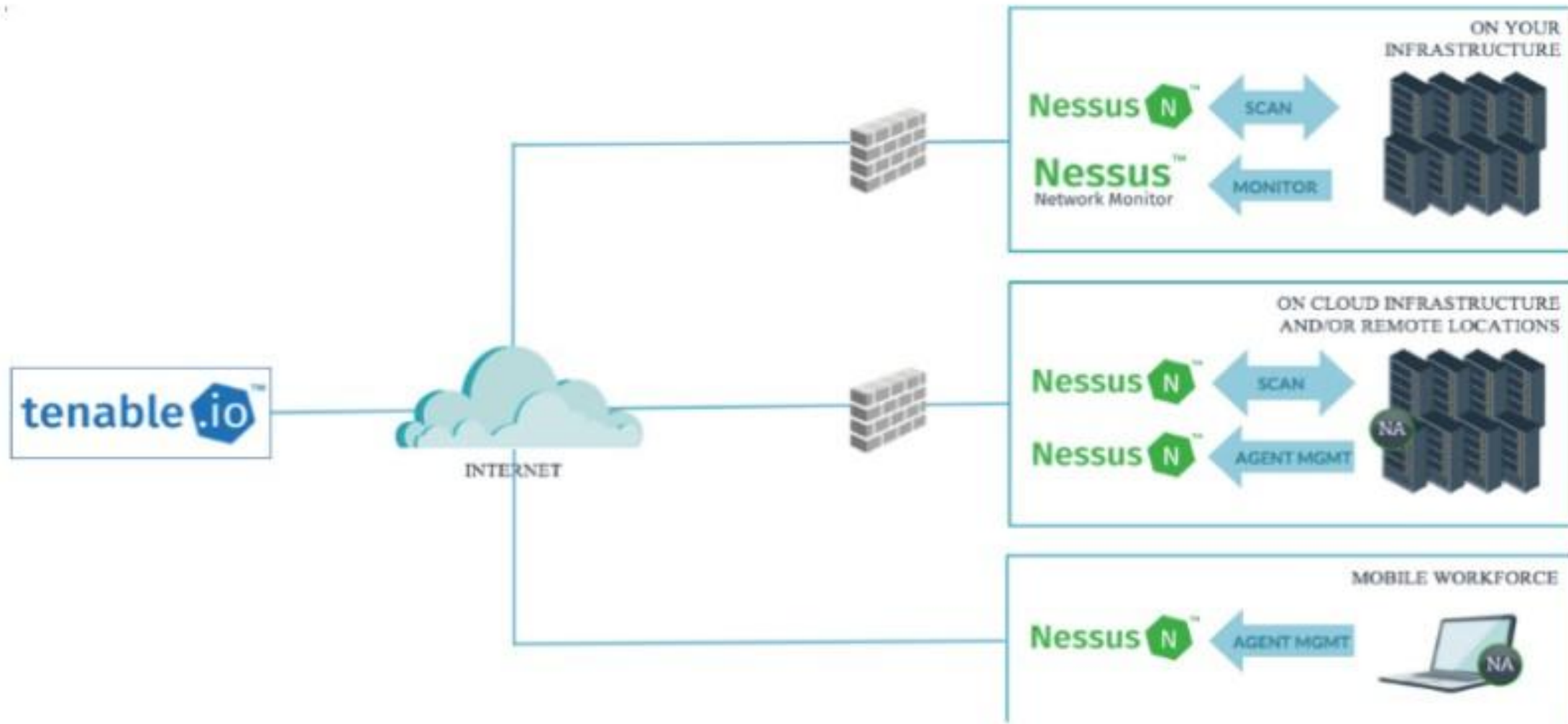
- **Nessus** เป็นโปรแกรมฟรีและเปิดรหัสสำหรับการตรวจหาช่องโหว่ในระบบเครือข่ายและไอที
- โปรแกรมนี้ใช้หลักการและอัลกอริทึมขั้นสูงในการค้นหาจุดอ่อนด้านความปลอดภัยในระบบคอมพิวเตอร์
- **Nessus** สามารถตรวจพบช่องโหว่ด้านรหัสโปรแกรมและการตั้งค่าระบบไอทีต่างๆ เพื่อปรับปรุงให้มั่นคงยิ่งขึ้น



License Comparison

	Nessus Essentials	Nessus Professional	Nessus Expert
เหมาะกับใคร	การเรียนรู้/ฝึกฝน การฝึกอบรม (การใช้งานที่ไม่ใช่เชิงพาณิชย์)	ที่ปรึกษาด้านความปลอดภัย องค์กรหรือทีมไอที ที่ต้องการการประเมินความปลอดภัยภายใน (Internal Threats) อย่างครอบคลุม	หน่วยงานหรือองค์กรขนาดใหญ่ที่ต้องการการประเมินความ ปลอดภัยขั้นสูง (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



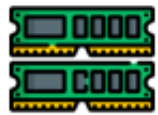
Hardware Requirements

Essential



2 Cores (Minimum)

4 Cores (Recommended)



4 GB (Minimum)

8 GB (Recommended)



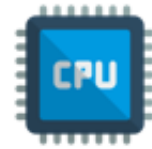
30 GB (Minimum)

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.

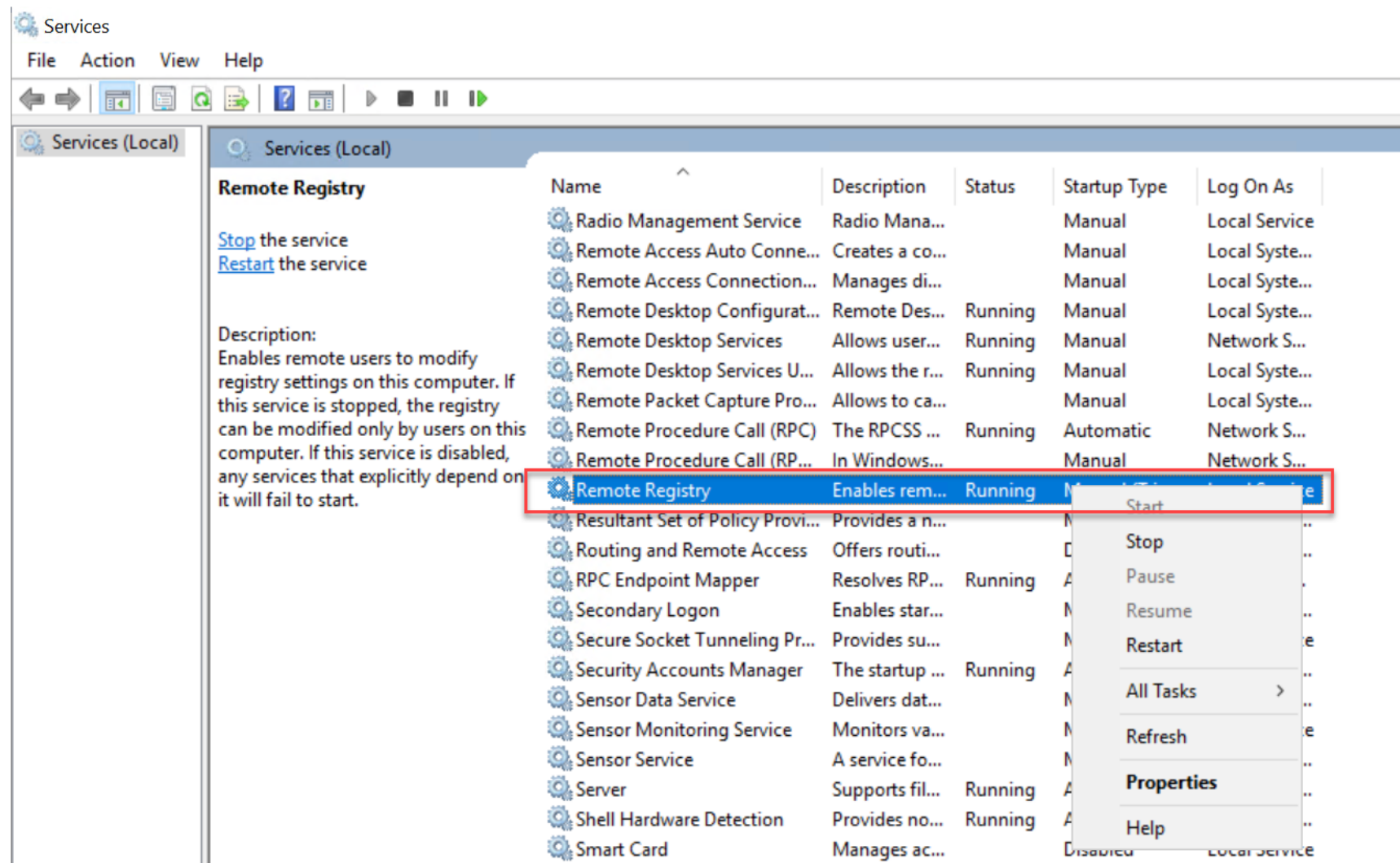
VULNERABILITIES

- **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.
-  **Mobile Device Scan**
Assess mobile devices via Microsoft Exchange or an MDM. *UPGRADE*
- **Web Application Tests**
Scan for published and unknown web vulnerabilities using Nessus Scanner.
- **Credentialed Patch Audit**
Authenticate to hosts and
- **Active Directory Starter Scan**
- **Find AI**
AI, LLM, ML related detections and

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

The screenshot shows the Windows Services console. The 'Services (Local)' window is open, displaying a list of services. The 'Windows Management Instrumentation' service is highlighted with a red box. A context menu is open over this service, showing options: Start, Stop, Pause, Resume, Restart, All Tasks >, Refresh, Properties, and Help. The service is currently 'Running'.

Name	Description	Status	Startup Type	Log On As
W3C Logging Service	Provides W...		Manual	Local Syste...
WalletService	Hosts objec...		Manual	Local Syste...
Windows Audio	Manages au...		Manual	Local Service
Windows Audio Endpoint Builder	Manages au...		Manual	Local Syste...
Windows Biometric Service	The Windo...		Automatic (T...	Local Syste...
Windows Camera Frame Server	Enables mul...		Manual (Trig...	Local Service
Windows Connection Manager	Makes auto...	Running	Automatic (T...	Local Service
Windows Defender Network Inspection Se...	Helps guard...		Manual	Local Service
Windows Defender Service	Helps prote...	Running	Automatic	Local Syste...
Windows Driver Foundation - User-mode ...	Creates and...	Running	Ma	
Windows Encryption Provider Host Service	Windows E...		Ma	
Windows Error Reporting Service	Allows error...		Ma	
Windows Event Collector	This service ...		Ma	
Windows Event Log	This service ...	Running	Aut	
Windows Firewall	Windows Fi...	Running	Aut	
Windows Font Cache Service	Optimizes p...	Running	Aut	
Windows Image Acquisition (WIA)	Provides im...		Ma	
Windows Insider Service	wisvc		Ma	
Windows Installer	Adds, modi...		Ma	
Windows License Manager Service	Provides inf...		Ma	
Windows Management Instrumentation	Provides a c...	Running	Aut	
Windows Mobile Hotspot Service	Provides th...		Manual (Trig...	Local Service
Windows Modules Installer	Enables inst...		Manual	Local Syste...

Scan Requirements

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

The screenshot shows the Windows Network and Sharing Center interface. The title bar reads "Network and Sharing Center". The breadcrumb navigation shows "Network and Internet > Network and Sharing Center". A search bar is present with the text "Search Control Panel".

On the left sidebar, the following options are listed:

- Control Panel Home
- Change adapter settings
- Change advanced sharing settings** (highlighted with a red box)

The main content area is titled "View your basic network information and set up connections". It displays "View your active networks" with a horizontal line. Below this, the network status is shown as:

- Network**: Private network
- Access type: No Internet access
- Connections: Ethernet0

Below the network status, there is a section titled "Change your networking settings" with a horizontal line. It contains two links:

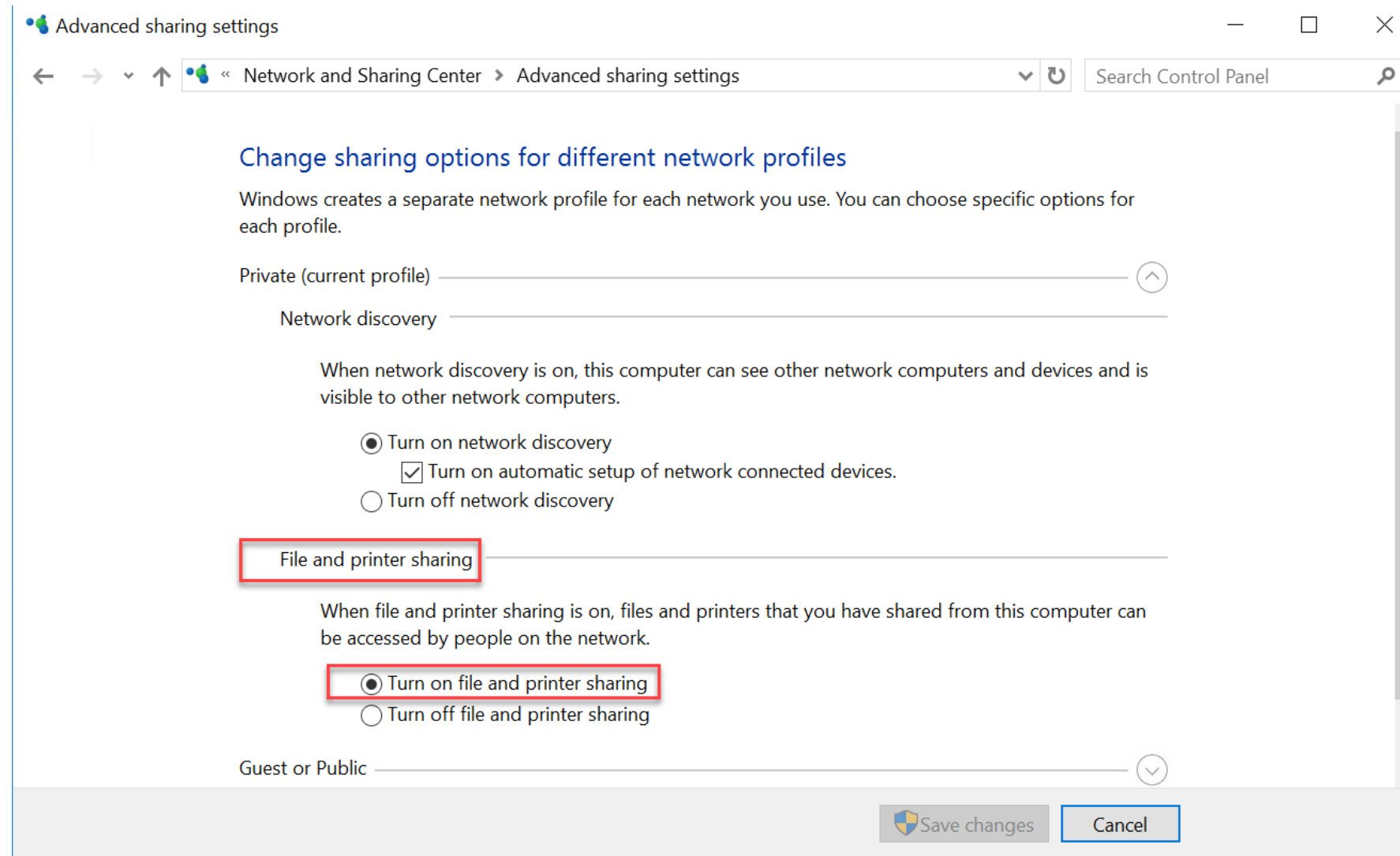
- Set up a new connection or network**: Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
- Troubleshoot problems**: Diagnose and repair network problems, or get troubleshooting information.

At the bottom left, under "See also", the following links are listed:

- Internet Options
- Windows Firewall

Scan Requirements

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

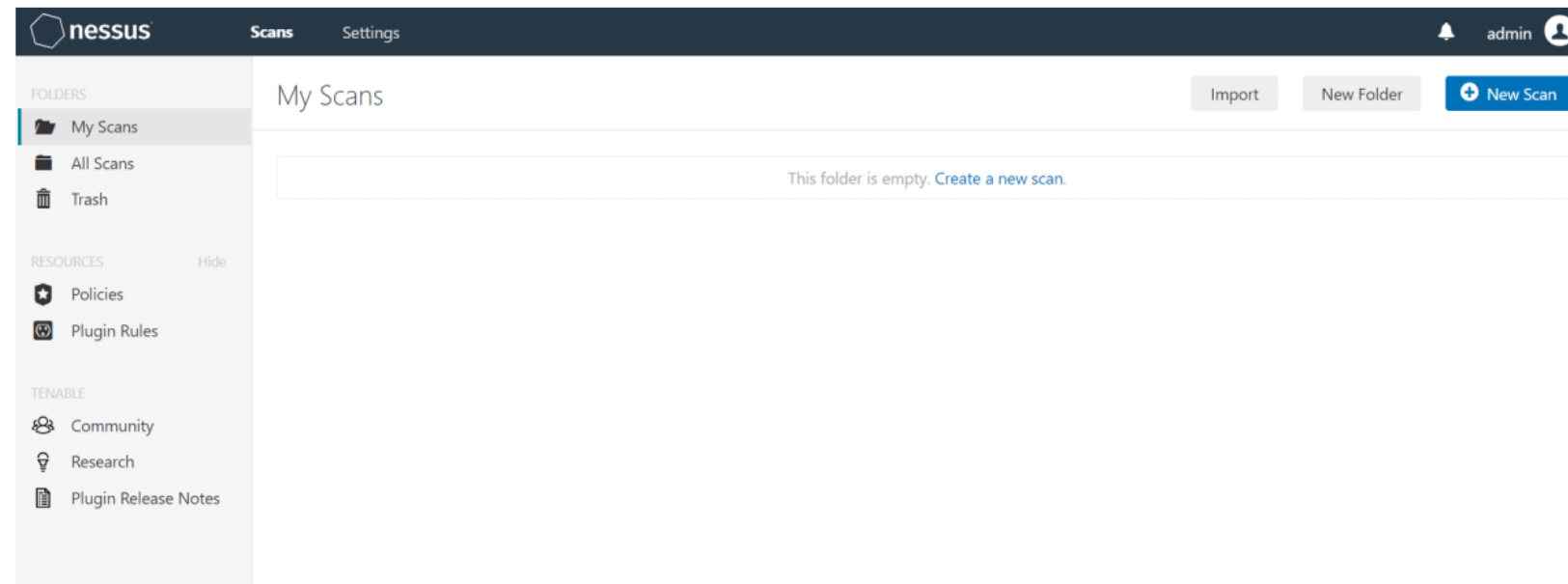


Create Scan

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
หากเครื่องปลายทางมีการตอบสนองกลับมาแปลว่าสแกนเจอเครื่องปลายทาง
เหล่านั้น โดย Policy ตัวนี้จะมีการสแกนที่ไวกว่า Policy ตัวอื่นๆเนื่องจากใช้
Pluginที่เกี่ยวข้องกับการค้นหาอุปกรณ์ปลายทางโดยเฉพาะ

Create Scan

The screenshot displays the Nessus Scan Templates interface. The top navigation bar includes the Nessus logo, 'Scans', and 'Settings' tabs, along with a user profile icon for 'admin'. A left sidebar contains navigation options: FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules), and FAVORITE (Community, Research, Plugin Release Notes). The main content area is titled 'Scan Templates' and includes a 'Back to Scans' link and a 'Scanner' dropdown menu set to 'User Defined'. A search bar is located in the top right of the main area.

The scan templates are organized into three main categories:

- DISCOVERY**: Includes 'Host Discovery' (highlighted with a red box), which is described as 'A simple scan to discover live hosts and open ports.'
- VULNERABILITIES**: A grid of 24 scan templates, including:
 - Basic Network Scan: A full system scan suitable for any host.
 - 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.
 - Mobile Device Scan: Assess mobile devices via Microsoft Exchange or an MDM. (UNUSABLE)
 - Web Application Tests: Scan for published and unknown web vulnerabilities.
 - Credentialed Patch Audit: Authenticate to hosts and enumerate missing updates.
 - Badlock Detection: Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
 - Bash Shellshock Detection: Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
 - DROWN Detection: Remote checks for CVE-2016-0800.
 - Intel AMT Security Bypass: Remote and local checks for CVE-2017-5888.
 - Shadow Brokers Scan: Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
 - Spectre and Meltdown: Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.
 - WannaCry Ransomware: Remote and local checks for MS17-010.
 - Ripple20 Remote Scan: A remote scan to fingerprint hosts potentially running the IIS stack in the network.
 - Zerologon Remote Scan: A remote scan to detect Microsoft Hologon (Elevation of Privilege) (Zerologon).
 - Solorigate: Remote and local checks to detect SolarWinds Solorigate vulnerabilities.
 - 2020 Threat Landscape Retrospective (TLR): A scan to detect vulnerabilities featured in our End of Year report.
 - ProxyLogon : MS Exchange: Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.
- COMPLIANCE**: Includes:
 - Audit Cloud Infrastructure: Audit the configuration of third-party cloud services.
 - Internal PCI Network Scan: Perform an internal PCI DSS (11.2.3) vulnerability scan.
 - MDM Config Audit: Audit the configuration of mobile device managers. (UNUSABLE)
 - Offline Config Audit: Audit the configuration of network devices.
 - PCI Quarterly External Scan: Approved for quarterly external scanning as required by PCI. (UNUSABLE)
 - Policy Compliance Auditing: Audit system configurations against a known baseline.
 - SCAP and OVAL Auditing: Audit systems using SCAP and OVAL definitions.

Create Scan

จากนั้นทำการใส่ข้อมูลในกรอบสีแดง

Name : ชื่อ Policy Scan ที่ต้องการตั้ง

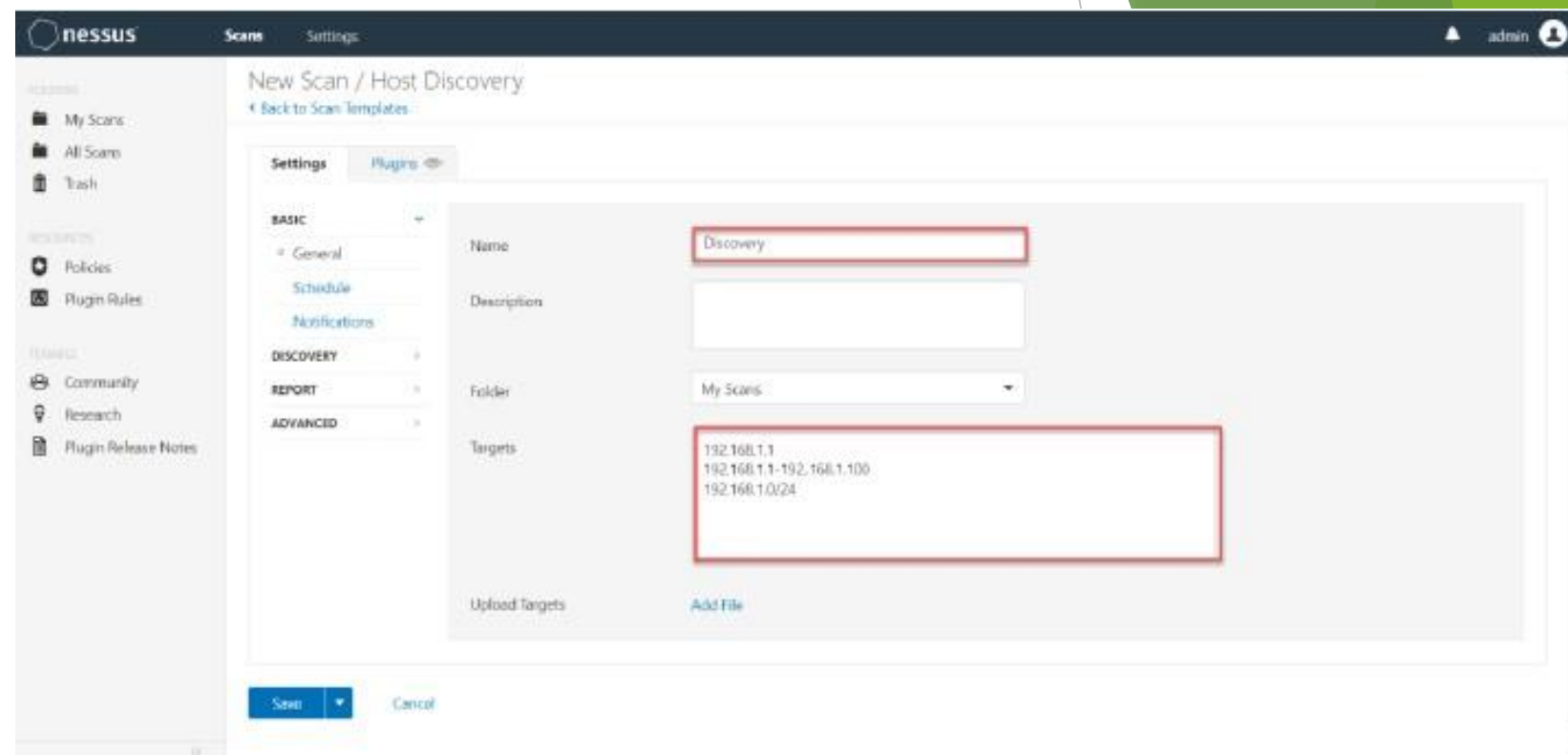
Target : ระบุเครื่องที่ต้องการสแกนด้วย IP Address ตามที่ต้องการ

โดยวิธีการระบุ IP สามารถระบุได้หลายแบบ เช่น

ทำการสแกน IP เดี่ยว 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



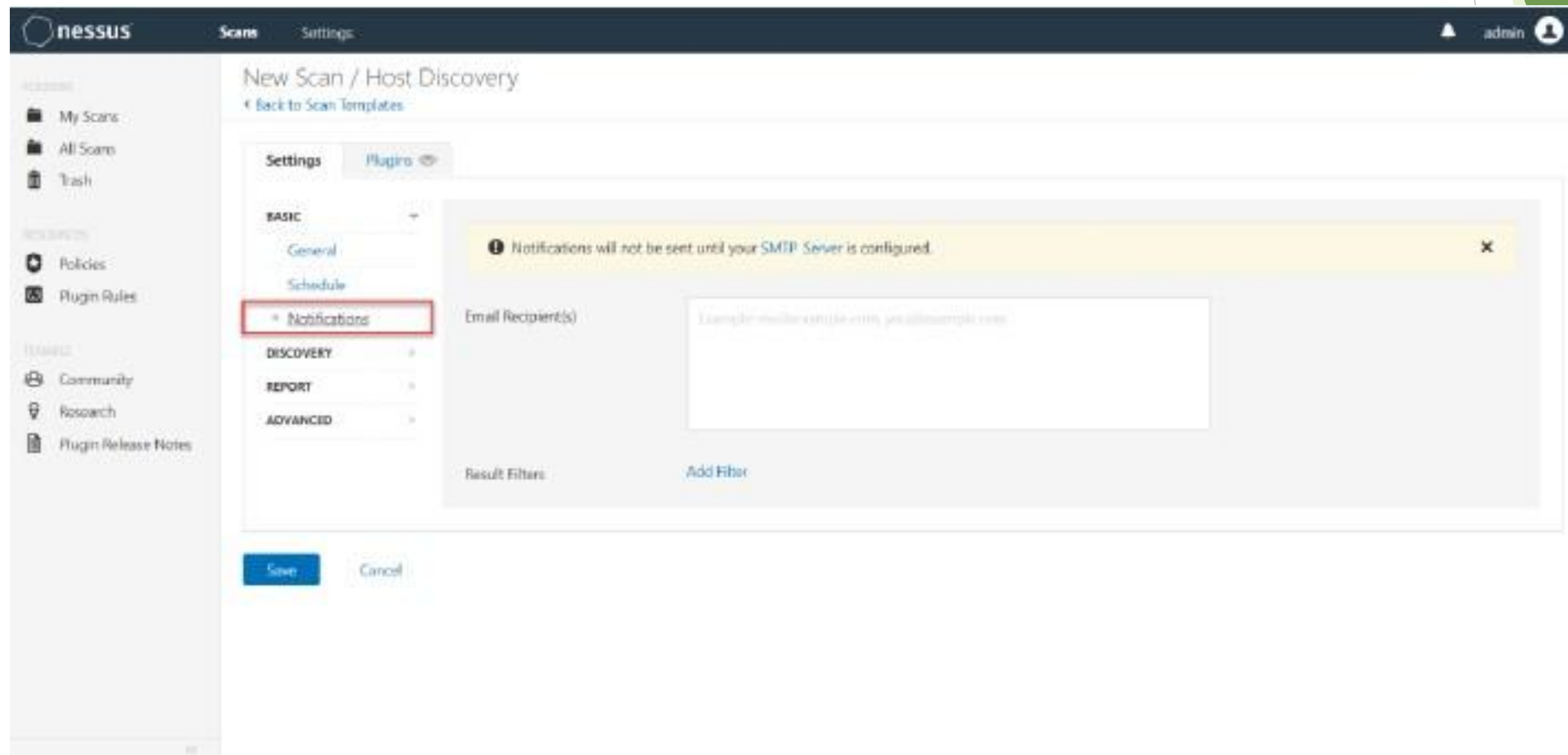
Create Scan

สามารถตั้ง Schedule ในการสแกนเป็น Daily , Weekly หรือ Monthly ได้

The screenshot shows the Nessus interface for creating a new scan. The left sidebar contains navigation options like 'My Scans', 'All Scans', 'Trash', 'Policies', and 'Plugin Rules'. The main content area is titled 'New Scan / Host Discovery' and has a 'Settings' tab selected. Under 'Settings', the 'Schedule' sub-tab is highlighted. The 'BASIC' section shows the scan is 'Enabled'. The 'Frequency' is set to 'Daily', 'Starts' at '13:30' on '2021-04-22', 'Timezone' is 'Asia/Bangkok', and 'Repeat Every' is 'Day'. A summary line indicates the scan will run 'Daily at 1:30 PM, starting on Thursday, April 22nd, 2021'. At the bottom, there are 'Save' and 'Cancel' buttons.

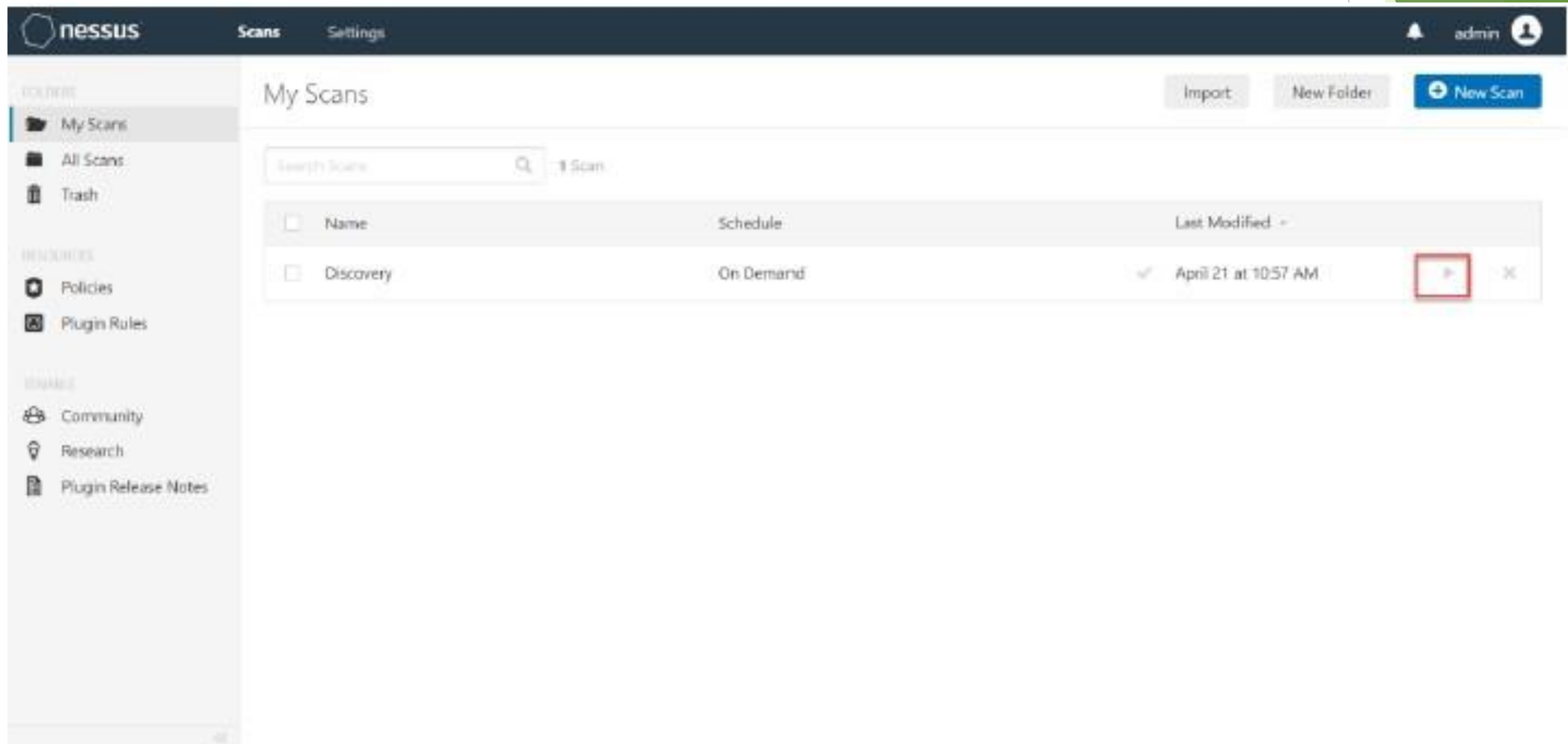
Create Scan

สามารถตั้ง Notifications แจ้งเตือนทาง Email หลังจากทำการสแกนเสร็จ โดยไม่จำเป็นต้องเชื่อมต่อกับ SMTP Server จากนั้นทำการกดปุ่ม Save เป็นอันเสร็จ



Create Scan

จะปรากฏ Policy ที่ใช้สำหรับการสแกนขึ้นมา จากนั้นทำการกดที่ปุ่มสามเหลี่ยมในกรอบสีแดง เพื่อทำการสั่งสแกน



Create Scan

ผลลัพธ์จะแสดงเกี่ยวกับเครื่องที่เจอ รวมถึง port ที่เปิดอยู่ของเครื่องนั้นๆ

The screenshot shows the Nessus web interface. The top navigation bar includes 'nessus', 'Scans', and 'Settings'. The user is logged in as 'admin'. The main content area is titled 'Discovery' and shows a list of discovered hosts and their open ports. A red box highlights the table containing the following data:

Host	Ports
10.2.2.1	22, 23, 80
10.2.2.57	22, 53, 161, 443, 4353
10.2.2.69	135, 139, 445, 1433, 2383, 3389, 49664, 49665, 49667, 49681, 49688, 4...
10.2.2.70	80, 135, 139, 443, 445, 1468, 1601, 2103, 2105, 2107, 3389, 4369, 6514, ...
10.2.2.100	80, 135, 139, 443, 445, 593, 1536, 1537, 1538, 1539, 1541, 1543, 1544, 1...
10.2.2.101	22
10.2.2.111	80, 443, 1433, 2383, 3389, 10001
10.2.2.134	80, 8443

On the right side of the interface, the 'Scan Details' section shows:

- Policy: Host Discovery
- Status: Completed
- Scanner: Local Scanner
- Start: April 21 at 10:50 AM
- End: April 21 at 10:57 AM
- Elapsed: 8 minutes

Below this, the 'Vulnerabilities' section features a donut chart showing the distribution of vulnerability severity levels: Critical, High, Medium, Low, and Info. The chart is currently empty, indicating no vulnerabilities were detected during this scan.

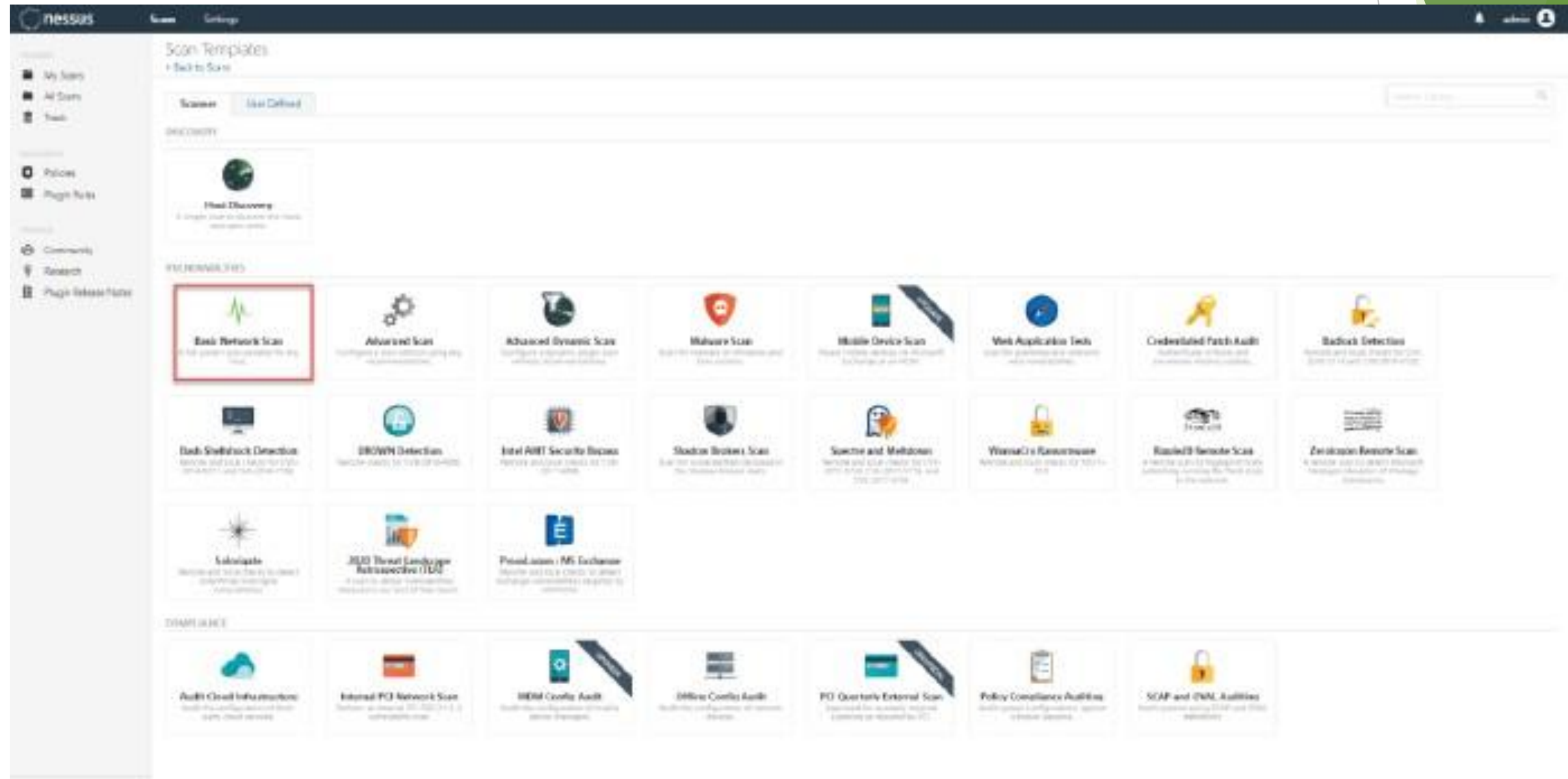
Create Scan

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 เดี่ยว 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

The screenshot shows the Nessus web interface for creating a new scan. The page title is "New Scan / Basic Network Scan". The left sidebar contains navigation options like "My Scans", "All Scans", "Trash", "Policies", "Plugin Rules", "Community", "Research", and "Plugin Release Notes". The main content area has tabs for "Settings", "Credentials", and "Plugins". Under the "Settings" tab, there are sections for "BASIC", "DISCOVERY", "ASSESSMENT", "REPORT", and "ADVANCED". The "BASIC" section is expanded, showing fields for "Name", "Description", "Folder", and "Targets". The "Name" field is filled with "Internal Network Scans". The "Folder" dropdown is set to "My Scans". The "Targets" field contains three entries: "192.168.1.1", "192.168.1.1-192.168.1.100", and "192.168.1.0/24". There is an "Add File" button next to the "Targets" field. At the bottom, there are "Save" and "Cancel" buttons.

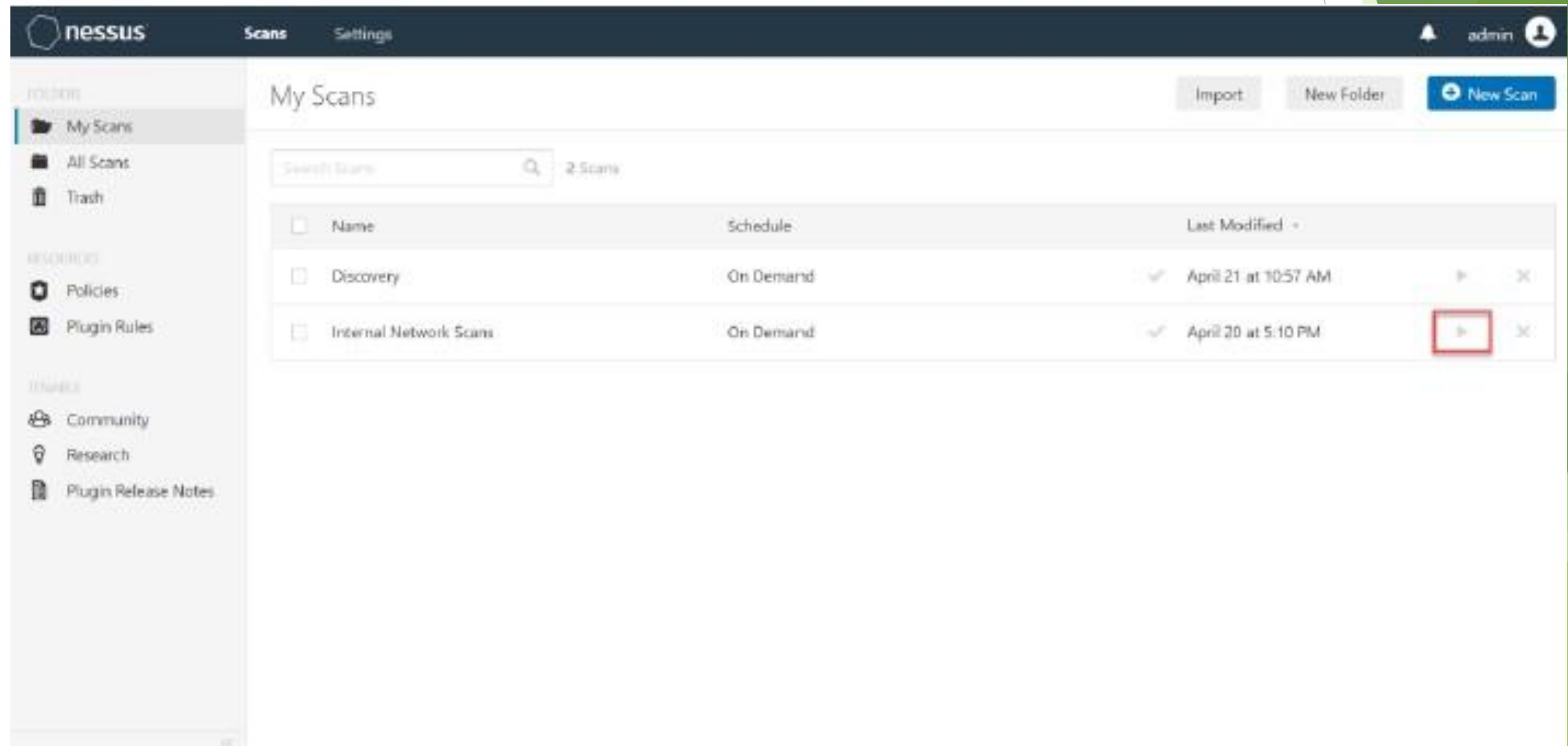
Create Scan

ทำการใส่ Credentials ของเครื่องปลายทางที่ต้องการสแกน

The screenshot displays the Nessus web interface for creating a new scan. The main heading is "New Scan / Basic Network Scan" with a "Back to Scan Templates" link. The "Credentials" tab is active, showing a list of categories: "Host", "SSH", and "Windows". The "Windows" category is selected. On the right, the "Authentication method" is set to "Password", and the "Username" is "administrator". The "Password" field is masked with asterisks. Below these fields, the "Global Credential Settings" section includes several checkboxes: "Never send credentials in the clear" (checked), "Do not use NTLMv1 authentication" (checked), and "Start the Remote Registry service during the scan" (unchecked).

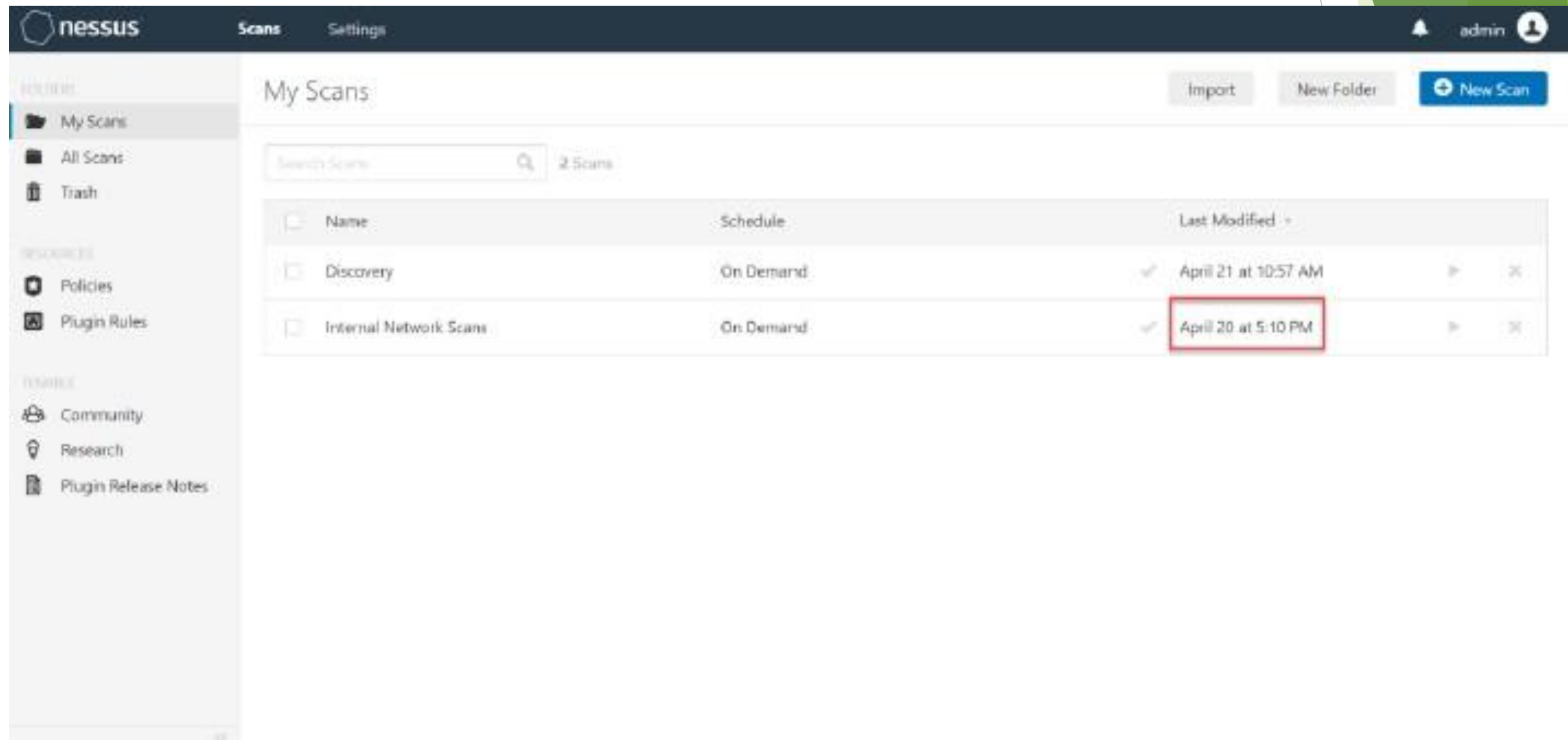
Create Scan

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



Create Scan

เมื่อทำการสแกนเสร็จ จะปรากฏข้อมูลตามภาพ ที่ทำการสแกนล่าสุด เป็นอันเสร็จ



The screenshot shows the Nessus web interface for managing scans. The main area is titled "My Scans" and contains a table with the following data:

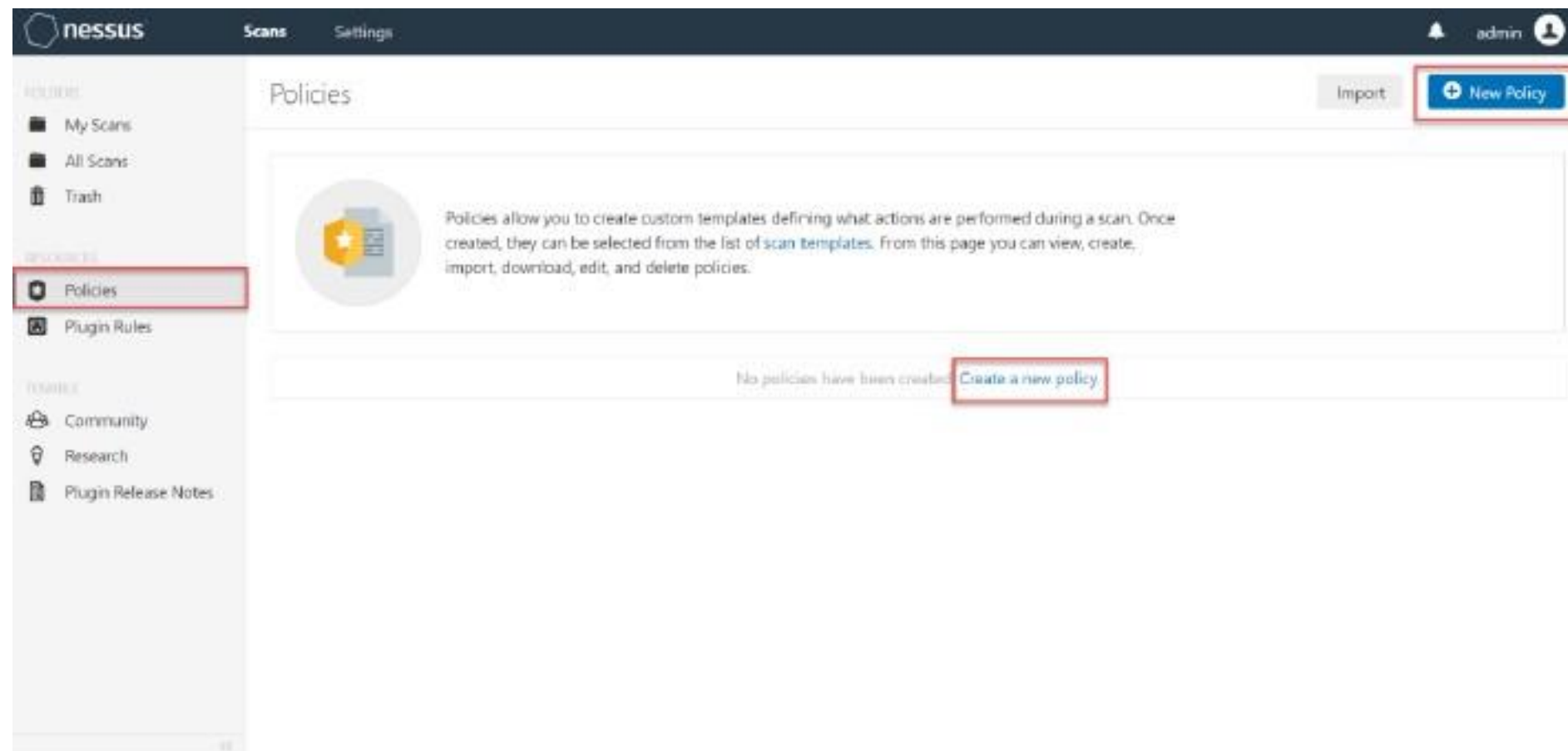
Name	Schedule	Last Modified
Discovery	On Demand	April 21 at 10:57 AM
Internal Network Scans	On Demand	April 20 at 5:10 PM

The "Last Modified" column for the "Internal Network Scans" entry is highlighted with a red box, indicating the most recent scan.

Policies

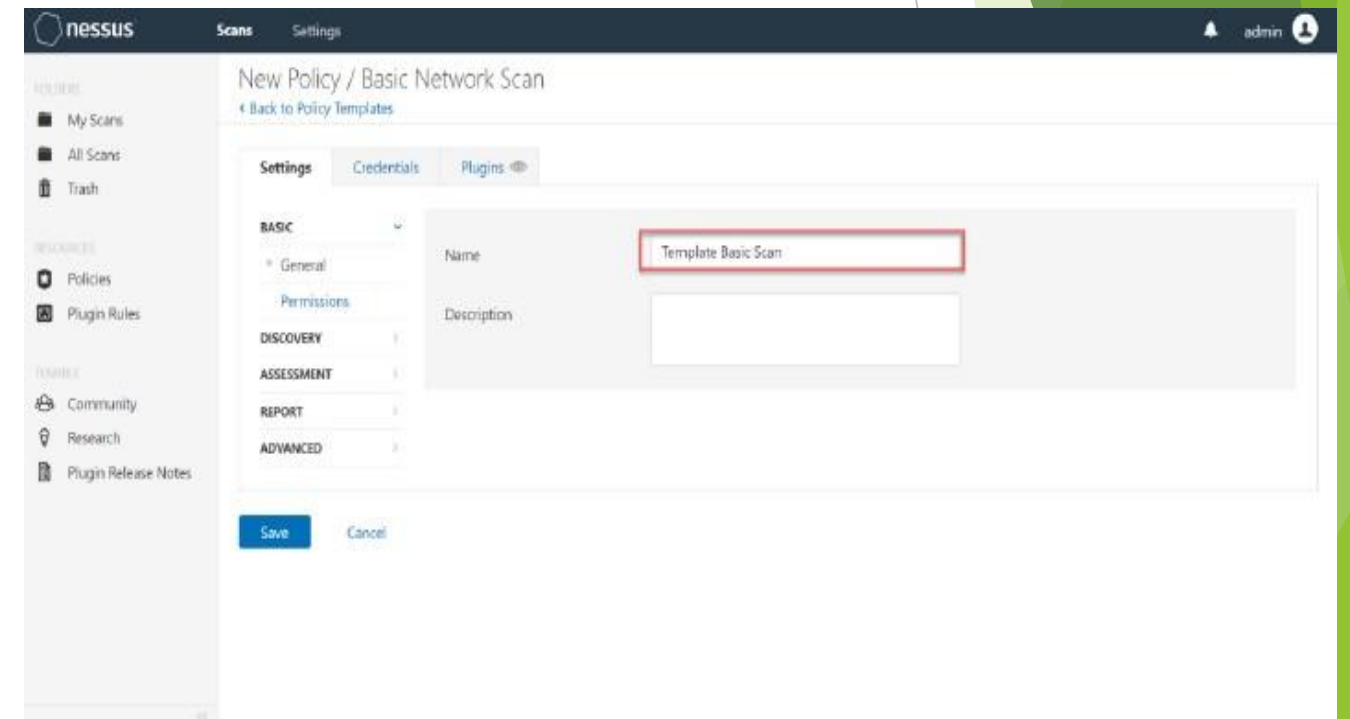
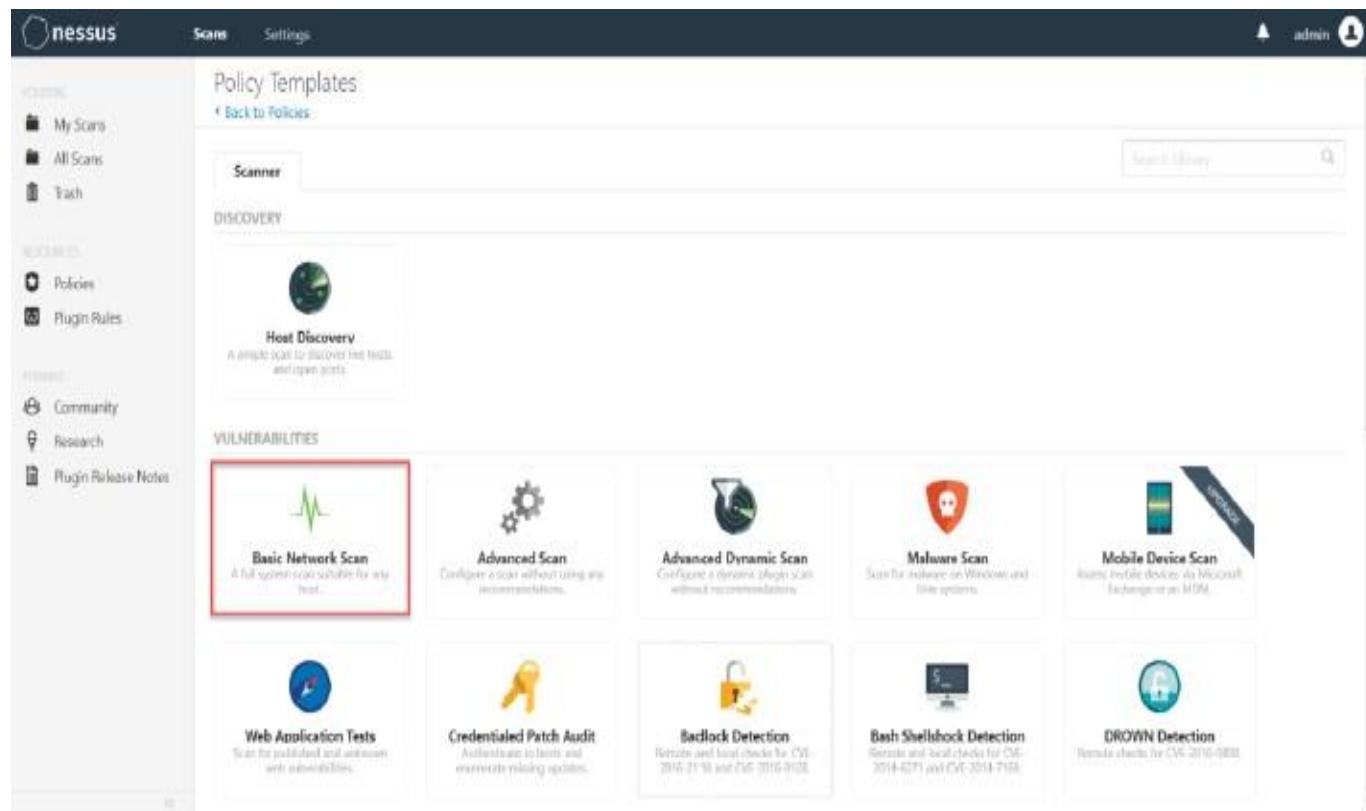
ในเมนูนี้สามารถสร้าง Policy ที่ใช้สำหรับการสแกนได้ ข้อดีคือสามารถใส่ตัว Credentials เป็น Template ไปได้ โดยไม่จำเป็นต้องใส่ Credentials ทุกครั้งที่สแกนใหม่

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



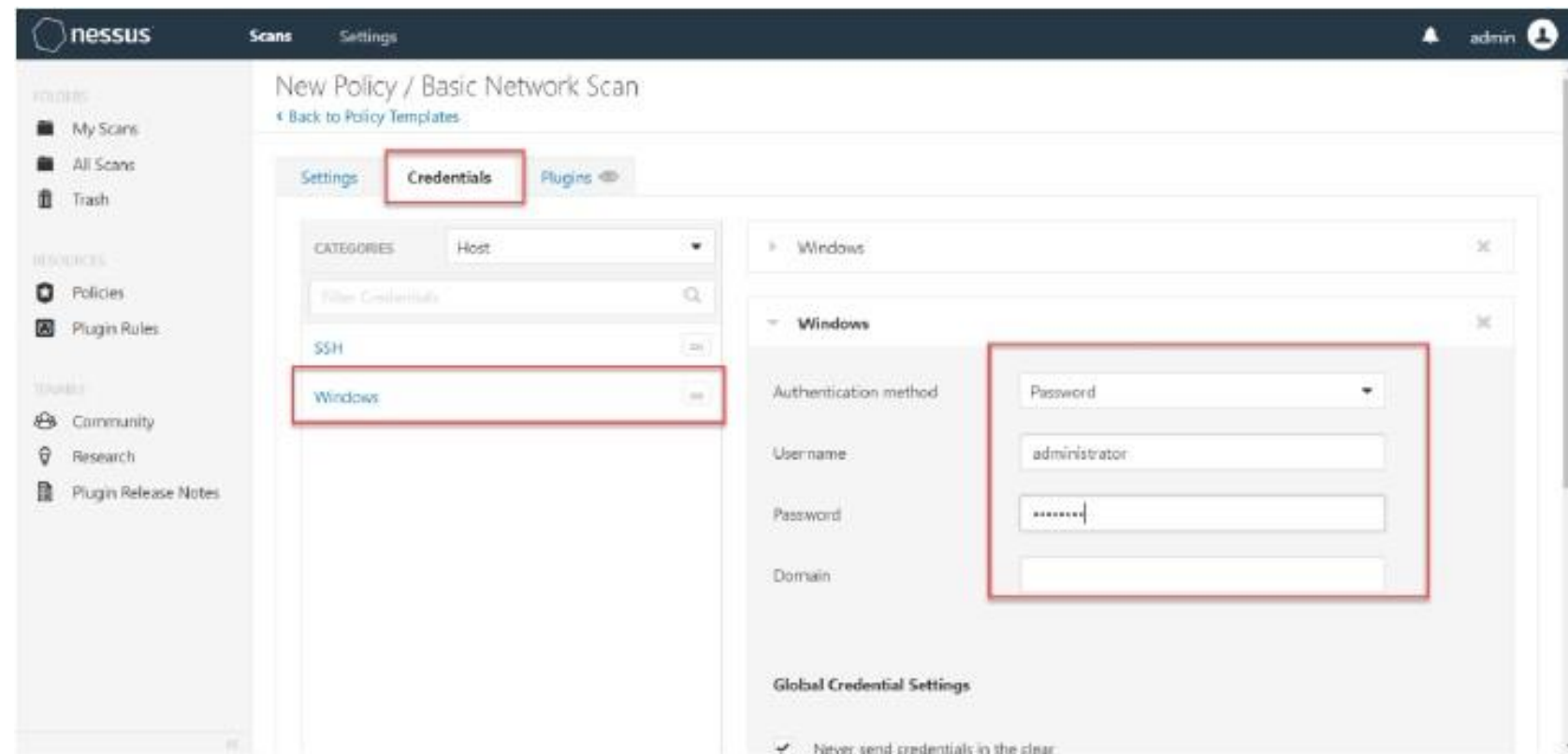
Policies

เลือก Policy Scan ที่ต้องการ เช่น Basic Network Scan แล้วใส่ชื่อ Template Policy



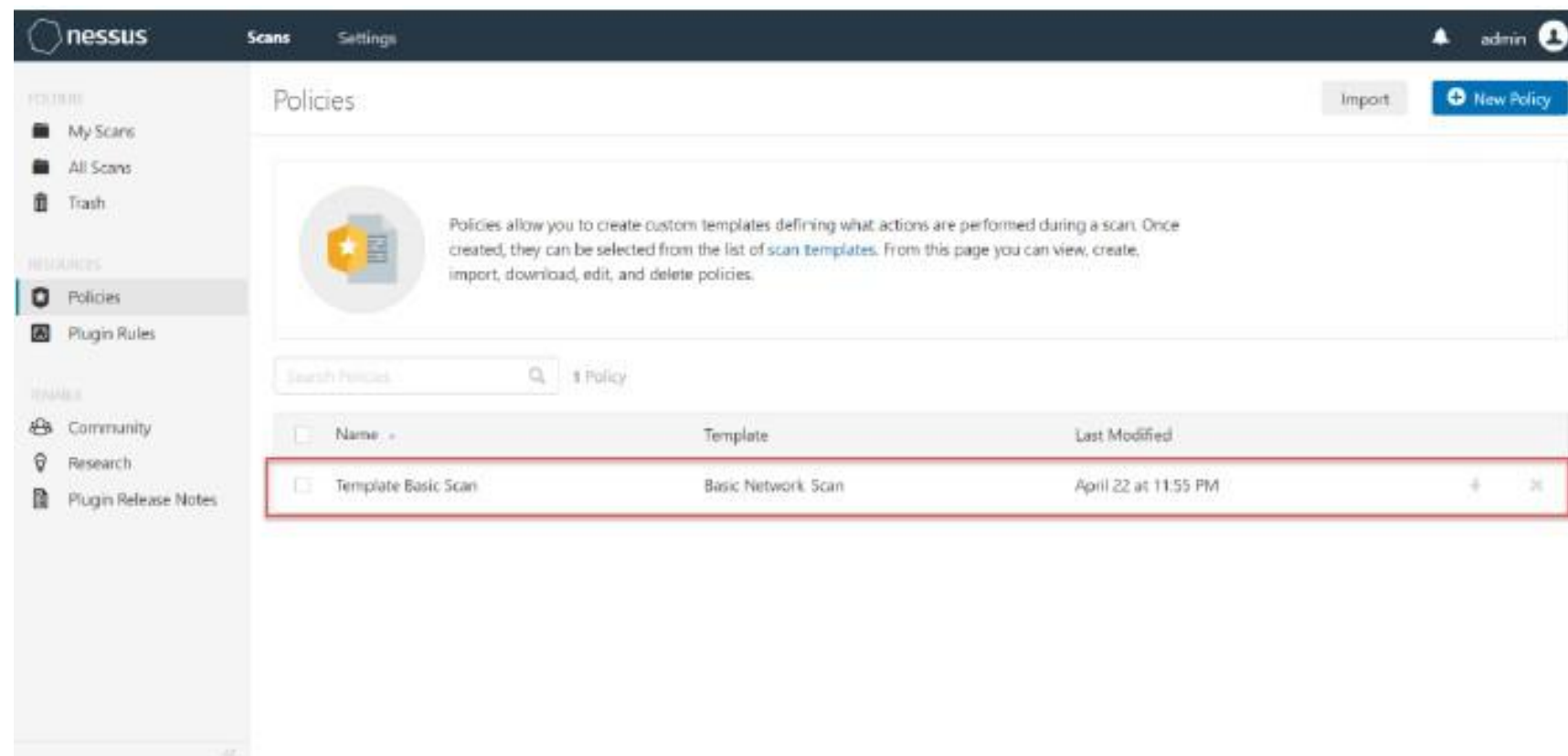
Policies

จากนั้นทำการใส่ Credentials สำหรับ Template Policy นี้ แล้วทำการกดปุ่ม Save เป็นอันเสร็จ



Policies

Template Policy ที่สร้างจะปรากฏขึ้นมา

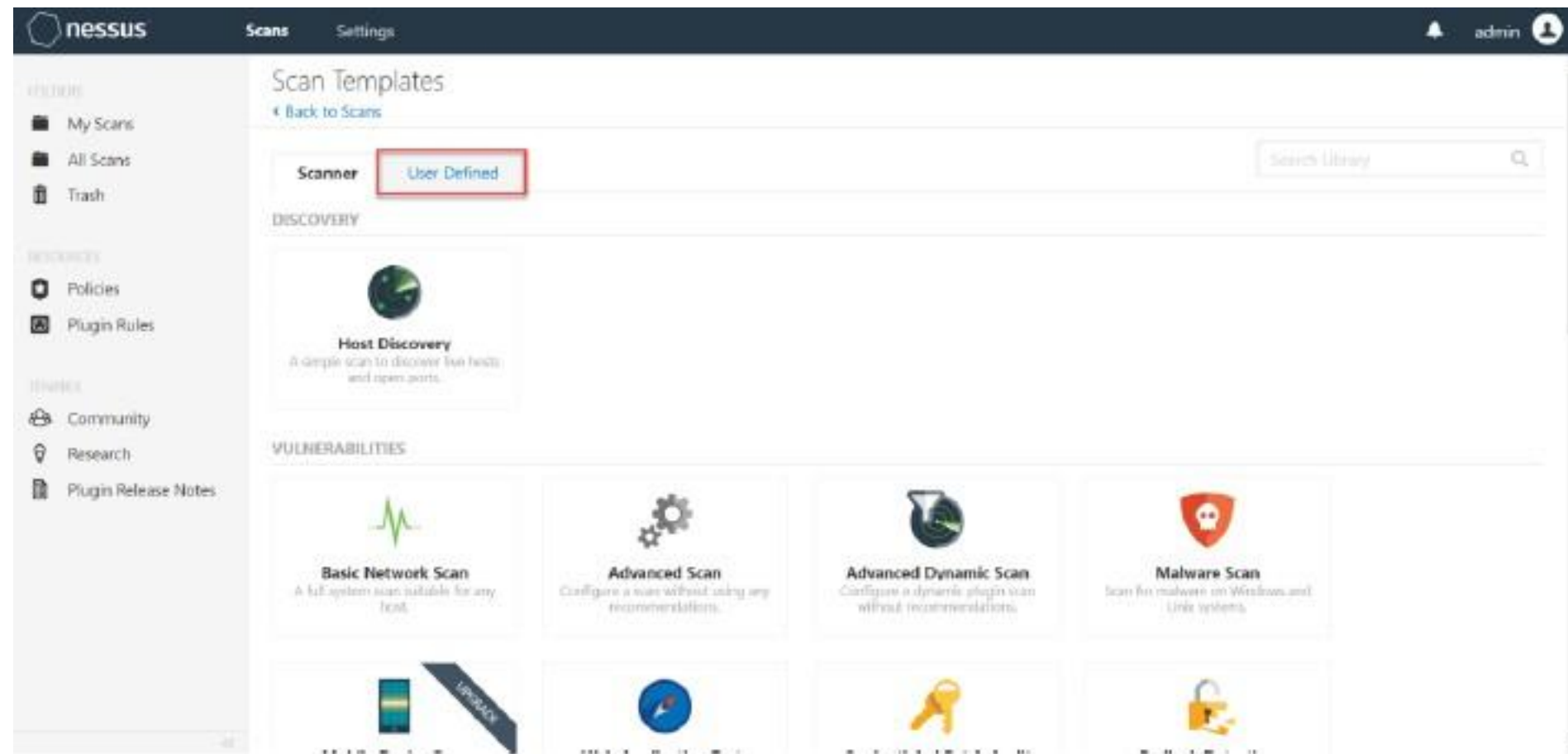


The screenshot shows the Nessus web interface for the Policies page. The top navigation bar includes the Nessus logo, 'Scans', and 'Settings' tabs, along with a user profile for 'admin'. The left sidebar contains navigation options: My Scans, All Scans, Trash, Policies (selected), Plugin Rules, Community, Research, and Plugin Release Notes. The main content area is titled 'Policies' and includes an 'Import' button and a '+ New Policy' button. A descriptive text box explains that policies allow creating custom templates for scan actions. Below this is a search bar for policies, showing '1 Policy' found. A table lists the policies with columns for Name, Template, and Last Modified. One policy is listed: 'Template Basic Scan' with the template 'Basic Network Scan' and a last modified date of 'April 22 at 11:55 PM'. The table row is highlighted with a red border.

<input type="checkbox"/>	Name	Template	Last Modified	
<input type="checkbox"/>	Template Basic Scan	Basic Network Scan	April 22 at 11:55 PM	+ -

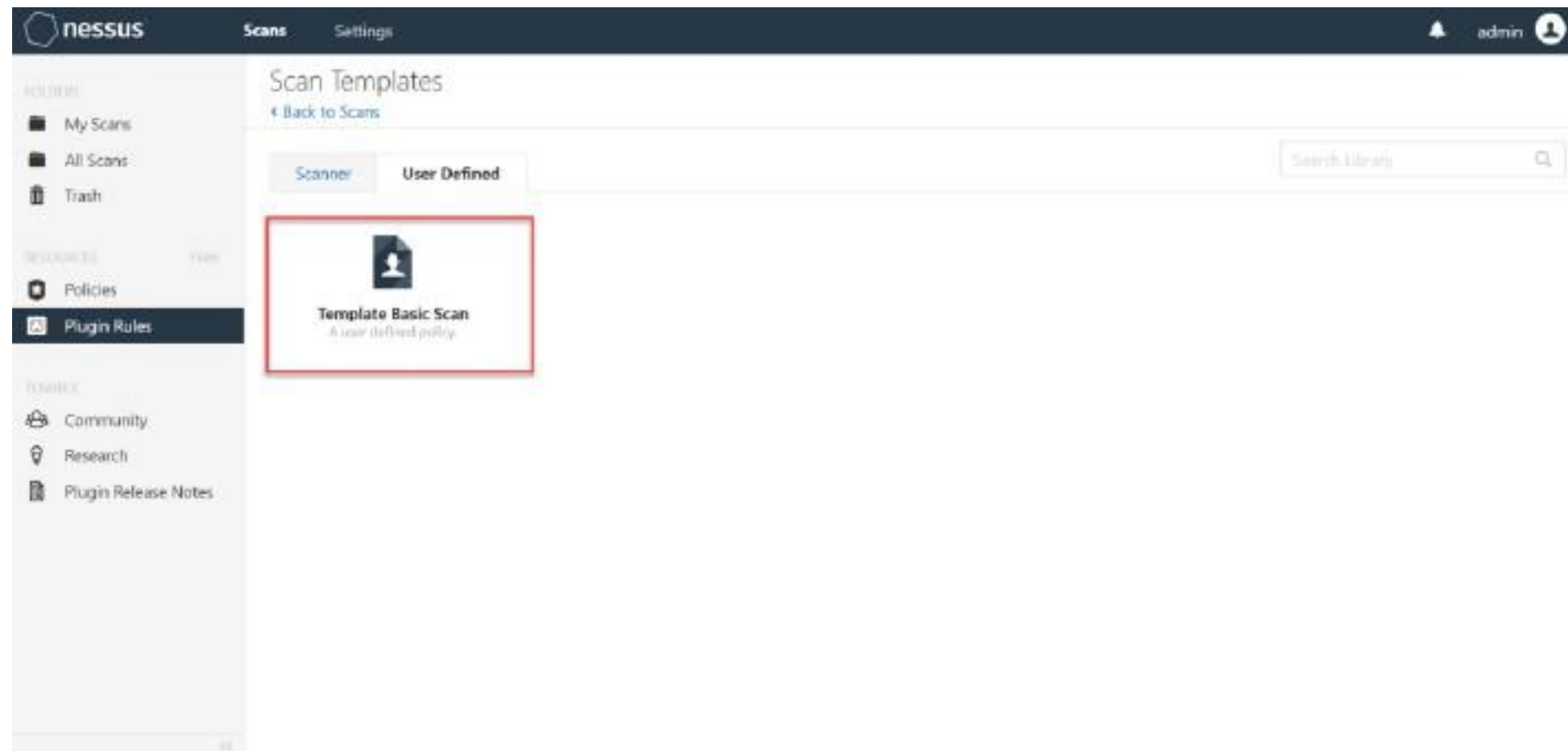
Policies

หากต้องการสแกนโดยใช้ Template ที่สร้างไว้ ให้ไปที่ New Scan เลือกหัวข้อ User Defined



Policies

เลือก Template ที่เราสร้างไว้



Policies

ทำการใส่ IP หรือตั้งค่า Schedule กับ Notifications จากนั้นทำการกดปุ่ม Save เป็นอันเสร็จ

The screenshot shows the Nessus web interface for configuring a new scan template. The page title is "New Scan / Template Basic Scan" with a "Back to Scan Templates" link. The left sidebar contains navigation options: "My Scans", "All Scans", "Trash", "Policies", "Plugin Rules", "Community", "Research", and "Plugin Release Notes". The main content area is titled "Settings" and includes a "BASIC" section with sub-tabs for "General", "Schedule", and "Notifications". The "General" tab is active, showing fields for "Name" (Template Basic Scan), "Description", "Folder" (My Scans), and "Targets". The "Targets" field is highlighted with a red box and contains the text: "Example: 192.168.1.1, 193.168.1.2, 192.168.2.2/24, localhost". Below the "Targets" field is an "Upload Targets" section with an "Add File" button.

การแปลผลและรายงานการตรวจสอบ

แสดงรายละเอียดของช่องโหว่

โปรแกรม Nexes จะแสดงรายละเอียดของช่องโหว่ที่พบ รวมถึงระดับความรุนแรงและผลกระทบ ซึ่งจะช่วยให้ผู้ดูแลระบบสามารถวิเคราะห์และจัดลำดับความสำคัญของการแก้ไข

จัดทำรายงานการตรวจสอบ

จัดทำรายงานการตรวจสอบแบบละเอียดครอบคลุมข้อมูลเกี่ยวกับช่องโหว่ที่พบผลกระทบ และแนวทางการแก้ไข เพื่อนำเสนอต่อผู้บริหาร

ประสานงานและดำเนินการแก้ไข

ประสานงานกับทีมงานเทคนิคเพื่อวางแผนและดำเนินการปิดช่องโหว่อย่างเป็นขั้นตอน เพื่อเพิ่มระดับความปลอดภัยระบบไอทีโดยรวม

Scan Result

ผลลัพธ์ของการสแกนแบบ Host Discovery จะบอกเครื่องและ Port ที่เจอของเครื่องนั้นๆ

The screenshot displays the Nessus interface for a Host Discovery scan. The main content area shows a table of discovered hosts and their open ports. The table is as follows:

Host	Ports
10.2.2.1	22, 23, 80
10.2.2.57	22, 53, 161, 443, 4353
10.2.2.69	135, 139, 445, 1433, 2383, 3389, 49664, 49665, 49667, 49681, 49688, 4...
10.2.2.70	80, 135, 139, 443, 445, 1468, 1801, 2103, 2105, 2107, 3389, 4369, 6514, ...
10.2.2.100	80, 135, 139, 443, 445, 593, 1536, 1537, 1538, 1539, 1541, 1543, 1544, 1...
10.2.2.101	22
10.2.2.111	80, 443, 1433, 2383, 3389, 10001
10.2.2.134	80, 8443

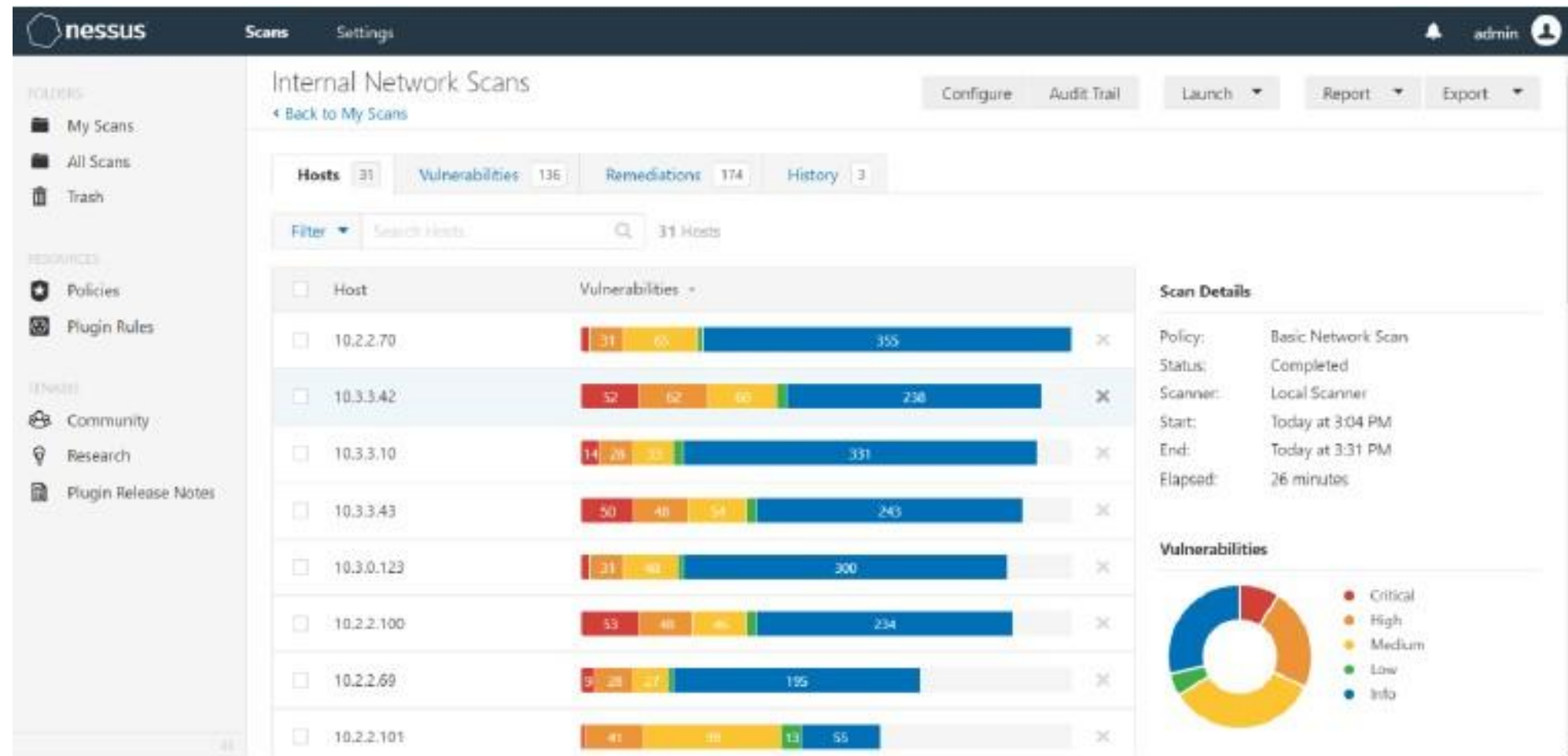
On the right side of the interface, the Scan Details section shows:

- Policy: Host Discovery
- Status: Completed
- Scanner: Local Scanner
- Start: April 21 at 10:50 AM
- End: April 21 at 10:57 AM
- Elapsed: 8 minutes

The Vulnerabilities section below it features a donut chart with a legend for severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The chart shows a single blue segment, indicating that all discovered vulnerabilities are of Info severity.

Scan Result

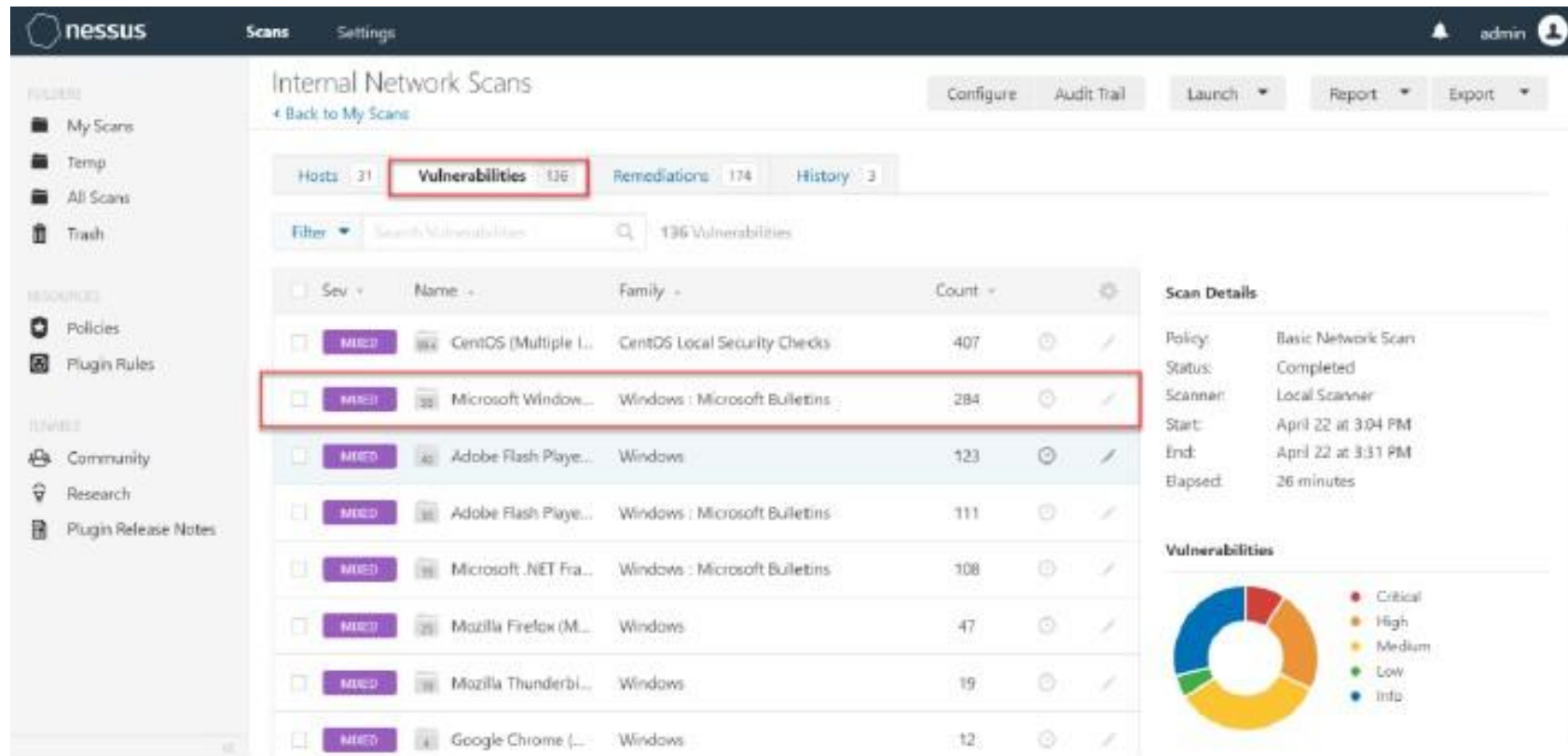
ผลลัพธ์ของการสแกนแบบ **Basic Network Scan** จะแสดงข้อมูลช่องโหว่ (Vulnerabilities) ระดับต่างๆที่เจอ



Troubleshooting

หลังจากทำการสแกนเสร็จ เราสามารถกดไปเข้าไปดูวิธีแก้ไขช่องโหว่ต่างๆได้

โดยทำการเลือก Policy Scan ที่ต้องการจะแก้ไขปัญหา > ไปที่เมนู Vulnerabilities แล้วเลือกช่องโหว่ที่ต้องการ



The screenshot displays the Nessus interface for 'Internal Network Scans'. The 'Vulnerabilities' tab is active, showing 136 vulnerabilities. A table lists the following vulnerabilities:

Sev	Name	Family	Count
MED	CentOS (Multiple L...	CentOS Local Security Checks	407
MED	Microsoft Window...	Windows : Microsoft Bulletin...	284
MED	Adobe Flash Playe...	Windows	123
MED	Adobe Flash Playe...	Windows : Microsoft Bulletin...	111
MED	Microsoft .NET Fra...	Windows : Microsoft Bulletin...	108
MED	Mozilla Firefox (M...	Windows	47
MED	Mozilla Thunderbi...	Windows	19
MED	Google Chrome (...)	Windows	12

Scan Details:

- Policy: Basic Network Scan
- Status: Completed
- Scanner: Local Scanner
- Start: April 22 at 3:04 PM
- End: April 22 at 3:31 PM
- Elapsed: 26 minutes

Vulnerabilities by Severity:

- Critical
- High
- Medium
- Low
- Info

Troubleshooting

เมื่อกดเข้ามา ก็จะเห็นรายละเอียด ของ Family Windows ตัวนี้ว่ามีช่องโหว่หรือ Plugin อะไรบ้างที่เกี่ยวข้อง
ให้ทำการเลือกช่องโหว่ที่ต้องการแก้ไข

The screenshot displays the Nessus interface for a scan titled "Internal Network Scans / Microsoft Windows (Multiple Is...". The interface includes a sidebar with navigation options like "My Scans", "Temp", "All Scans", and "Trash". The main content area shows a table of vulnerabilities with columns for severity, name, family, and count. One vulnerability, KB5001633, is highlighted with a red box. To the right, there is a "Scan Details" section and a "Vulnerabilities" donut chart.

Sev	Name	Family	Count
CRITICAL	KB4534271: Windows 1...	Windows : Microsoft Bulletins	7
CRITICAL	KB4540670: Windows 1...	Windows : Microsoft Bulletins	7
CRITICAL	KB4566830: Windows 1...	Windows : Microsoft Bulletins	7
CRITICAL	KB5000803: Windows 5...	Windows : Microsoft Bulletins	7
CRITICAL	KB5001347: Windows 1...	Windows : Microsoft Bulletins	7
CRITICAL	KB5001633: Mar 2021 ...	Windows : Microsoft Bulletins	7
CRITICAL	KB4534273: Windows 1...	Windows : Microsoft Bulletins	1
CRITICAL	KB4538461: Windows 1...	Windows : Microsoft Bulletins	1

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Scanner: Local Scanner
- Start: April 22 at 3:04 PM
- End: April 22 at 3:31 PM
- Elapsed: 26 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Troubleshooting

ข้อมูลต่างๆเกี่ยวกับ Plugin ตัวนี้จะปรากฏขึ้นมาดังนี้

Description : จะบอกรายละเอียดเกี่ยวกับช่องโหว่ตัวนี้

Solution : วิธีแก้ไขช่องโหว่ตัวนี้

See Also : รายละเอียดเพิ่มเติมเกี่ยวกับช่องโหว่ตัวนี้

Plugin Details : ข้อมูลเกี่ยวกับช่องโหว่

Risk Information : ข้อมูล Score ของช่องโหว่ตัวนี้

The screenshot shows the Nessus interface for a specific vulnerability. The main content area displays the following information:

- Severity:** Critical
- ID:** 148482
- Version:** 1.3
- Type:** local
- Family:** Windows - Microsoft Bulletins
- Published:** April 13, 2021
- Modified:** April 15, 2021

Description: The remote Windows host is missing an out-of-band security update. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution: Microsoft has released KB5001633 to address this issue.

See Also: <https://support.microsoft.com/en-us/help/5001633>

Output: The remote host is missing one of the following rollup KBs :
- 5001633
C:\Windows\system32\ntoskrnl.exe has not been patched.
Remote version : 10.0.14393.2948
Should be : 10.0.14393.4283

Risk Information: Risk Factor: Critical
CVSS v3.0 Base Score: 9.8
CVSS v3.0 Vector: CVSS:3.0/AW/N/ACL/PRN/UI/MSU/C/H/HA/H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 8.5
CVSS Base Score: 10.0

Report

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

The screenshot shows the Nessus web interface. The top navigation bar includes the Nessus logo, 'Scans', and 'Settings' tabs. The user is logged in as 'admin'. The main heading is 'Internal Network Scans'. Below this, there are buttons for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. The 'Report' dropdown menu is open, showing options for 'PDF', 'HTML', and 'CSV'. The main content area displays a table of hosts with their vulnerability counts and a donut chart showing the distribution of vulnerability severity levels.

Host	Vulnerabilities
10.2.2.70	355
10.3.3.42	230
10.3.3.10	331
10.3.3.43	243
10.3.0.123	301
10.2.2.100	234
10.2.2.69	195
10.2.2.101	55

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 3:04 PM
- End: Today at 3:31 PM
- Elapsed: 26 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Report

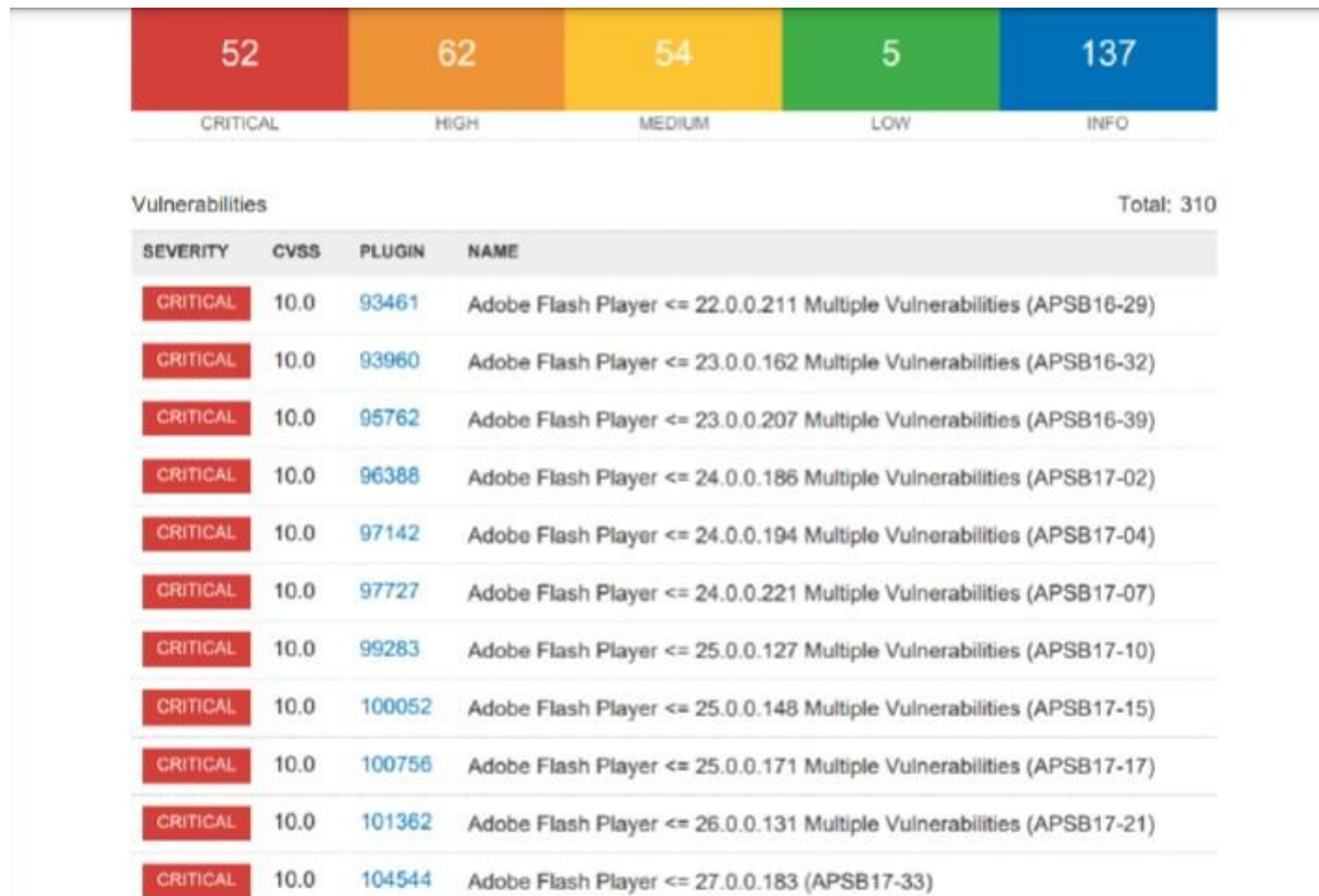
ประเภทข้อมูลของ Report จะมีให้เลือก 2 แบบคือ Executive Summary และ Custom



The image shows a software interface for generating a PDF report. The main window is titled "Generate PDF Report" and has a close button (X) in the top right corner. Inside the window, there is a label "Report" followed by a dropdown menu. The dropdown menu is open, showing three options: "Executive Summary" (with a small upward-pointing triangle), "Executive Summary" (highlighted with a grey background), and "Custom". Below the dropdown menu, there are two buttons: a blue button labeled "Generate Report" and a grey button labeled "Cancel".

Report

ตัวอย่าง Report แบบ Executive Summary



Report

ตัวอย่าง Report แบบ Custom

Generate PDF Report - 2 Hosts Selected

Report: Custom

Data:
 Vulnerabilities
 Remediations

Group Vulnerabilities By: Host

Scan Information
 Host Information

Vulnerabilities Details Select All | Clear

<input checked="" type="checkbox"/> Synopsis	<input checked="" type="checkbox"/> CVSS Base Score
<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> CVSS Temporal Score
<input checked="" type="checkbox"/> See Also	<input checked="" type="checkbox"/> STIG Severity
<input checked="" type="checkbox"/> Solution	<input checked="" type="checkbox"/> References
<input checked="" type="checkbox"/> Risk Factor	<input checked="" type="checkbox"/> Exploitable With
<input checked="" type="checkbox"/> CVSS v3.0 Base Score	<input checked="" type="checkbox"/> Plugin Information
<input checked="" type="checkbox"/> CVSS v3.0 Temporal Score	<input checked="" type="checkbox"/> Plugin Output

Some vulnerability details do not exist in all results

Formatting Options
 Include page breaks between vulnerability results

Save as default

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

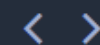
The version of Adobe Flash Player installed on the remote Windows host is equal or prior to version 22.0.0.211. It is, therefore, affected by multiple vulnerabilities :

- 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



Plugin Details



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
```

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



Plugin Details

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>

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



Plugin Details

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

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 behaviour 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

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

อัปเดตซอฟต์แวร์, เปลี่ยนรหัสผ่าน
และ จำกัดการเข้าถึงข้อมูล

2

ติดตั้งระบบและเครื่องมือรักษา
ความปลอดภัย

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

3

จัดทำแผนรับมือและซ้อมแผนรับมือ

เพื่อทันต่อเหตุการณ์ที่อาจเกิดขึ้นทาง
ไซเบอร์อย่างต่อเนื่อง



สรุปและแนะนำแนวทางปฏิบัติ

ช่วยตรวจพบจุดอ่อน

การใช้โปรแกรม Nexes ช่วยให้สามารถตรวจพบจุดอ่อนในระบบไอทีเบื้องต้นได้อย่างมีประสิทธิภาพ และเป็นจุดเริ่มต้นในการยกระดับความปลอดภัยทางไซเบอร์อย่างเป็นระบบ

ปิดช่องโหว่อย่างต่อเนื่อง

แนะนำให้องค์กรสำรวจและ ปิดช่องโหว่ที่พบอย่างต่อเนื่อง ควบคู่กับการจัดทำนโยบายและแผนบริหารความเสี่ยงด้านไซเบอร์อย่างเป็นรูปธรรม

The background features abstract, overlapping geometric shapes in various shades of green, ranging from light lime to dark forest green. These shapes are primarily located on the left and right sides of the slide, framing the central text. The overall aesthetic is clean and modern.

Thankyou

Q&A