

HƯỚNG DẪN CÀI ĐẶT VÀ SỬ DỤNG CÁC CÔNG CỤ HỖ TRỢ CHO QUÁ TRÌNH DIỄN TẬP

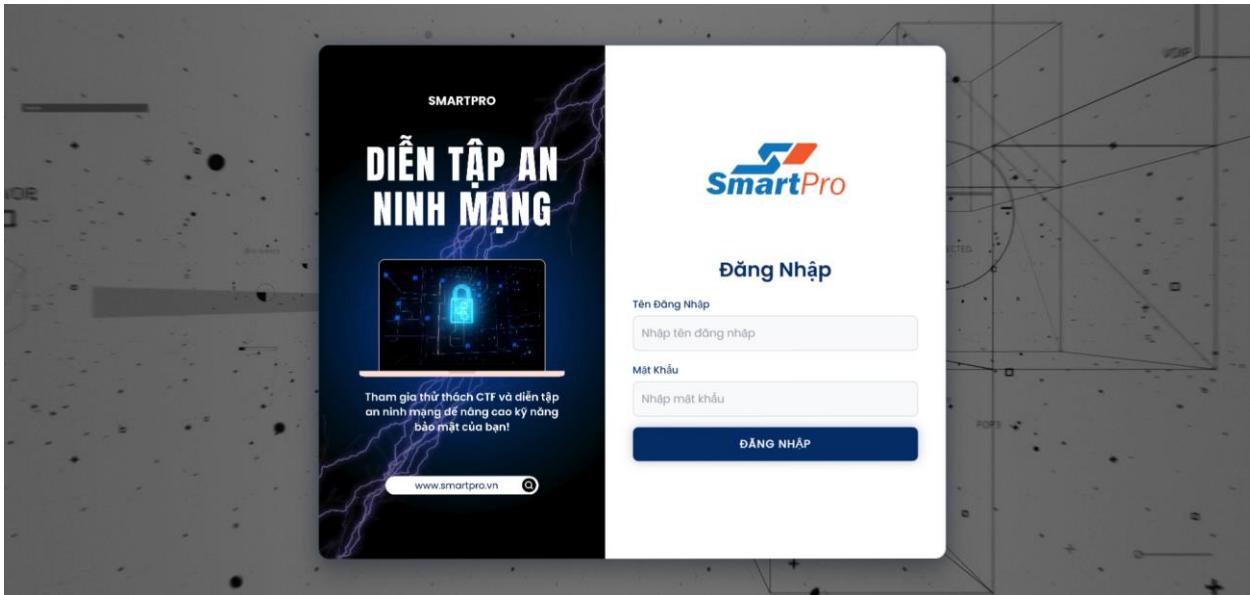
(WireShark + Ultraviewer + Ivanti Security Controls + GoPhish)

1. Mục tiêu:

Tài liệu này nhằm cung cấp một lộ trình rõ ràng và chi tiết để người dùng có thể cài đặt, cấu hình và vận hành hiệu quả các công cụ này trong các kịch bản diễn tập. Tài liệu nhằm hỗ trợ người sử dụng hiểu rõ chức năng của từng công cụ - WireShark để phân tích mạng, Ultraviewer để điều khiển từ xa, Ivanti Security Controls để quản lý bảo mật, và GoPhish để mô phỏng tấn công lừa đảo - từ đó tối ưu hóa quá trình thực hành, nâng cao kỹ năng và đảm bảo an toàn thông tin trong môi trường mô phỏng.

2. Hướng dẫn truy cập vào hệ thống:

- Truy cập vào đường dẫn: <https://submit.smartpro.edu.vn/> sau đó đăng nhập vào tài khoản đã được cung cấp



- Sau khi đã đăng nhập thành công, ta chọn: “**Công cụ → Tất Cả**”

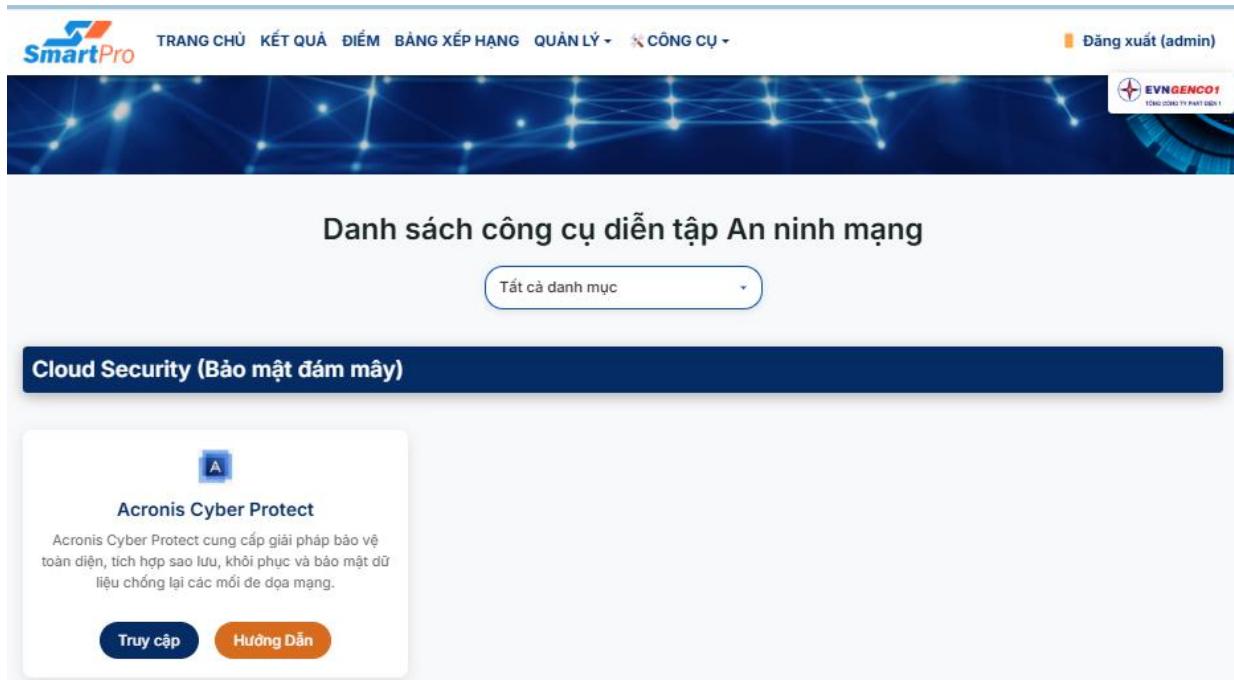


The screenshot shows the SmartPro web interface. At the top, there is a navigation bar with links: TRANG CHỦ, KẾT QUẢ, ĐIỂM, BÀNG XẾP HẠNG, QUẢN LÝ, CÔNG CỤ (with a dropdown arrow), and Đăng xuất (admin). The main banner features the text "CHƯƠNG TRÌNH DIỄN TẬP THỰC CHIẾN BẢO ĐẢM AN NINH MẠNG EVNGENCO1 2025". A red box highlights the "CÔNG CỤ" dropdown menu, and a red arrow points to the "Tất cả" option within it.

Danh sách thử thách

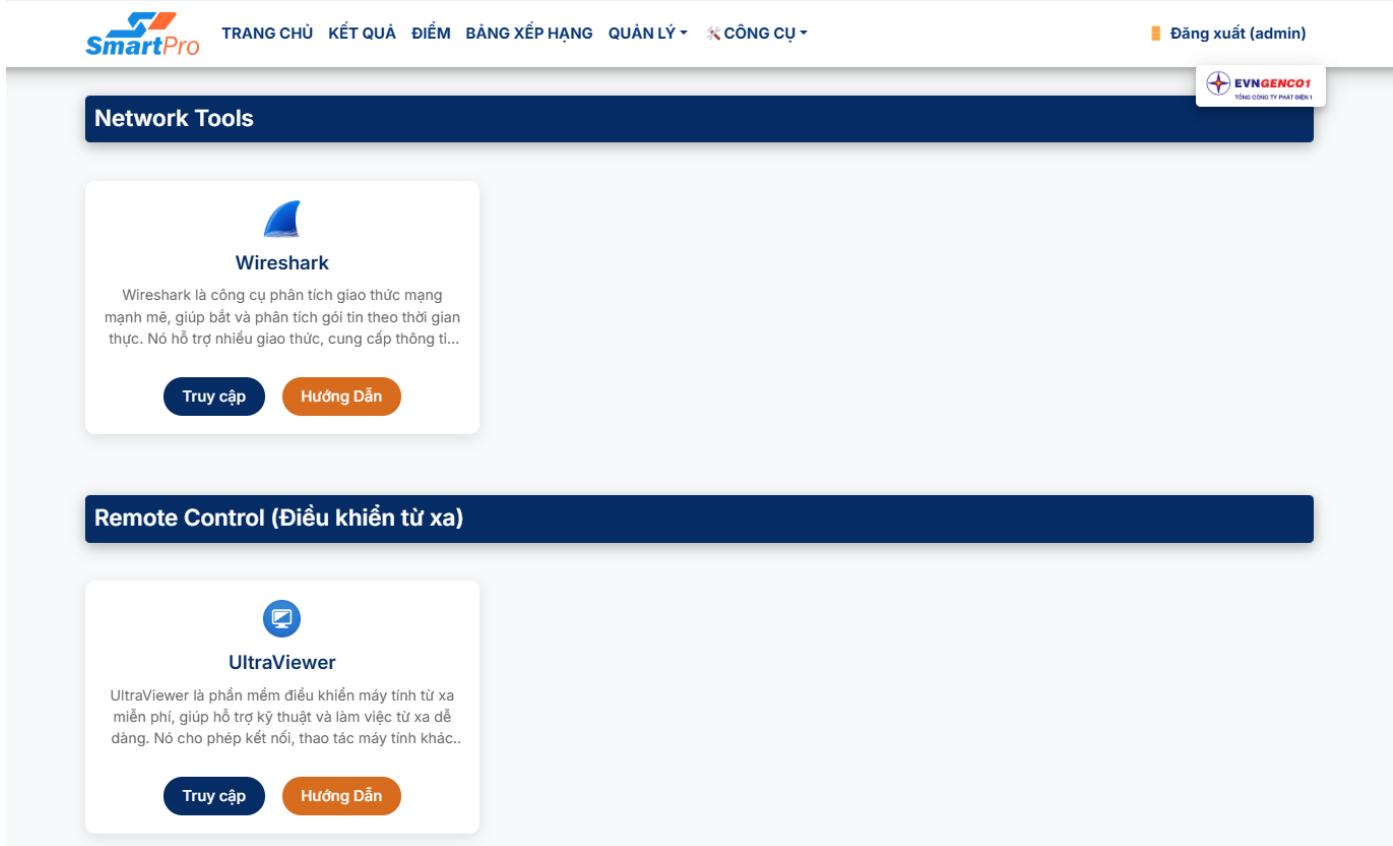
Tiến độ: 3 / 8 thử thách hoàn thành

- Ta sẽ thấy được “Danh sách các công cụ” và Danh Mục của chúng



The screenshot shows the "Danh sách công cụ" section for "Cloud Security (Bảo mật đám mây)". The page title is "Danh sách công cụ diễn tập An ninh mạng". Below the title is a dropdown menu with the option "Tất cả danh mục". The main content area displays a card for "Acronis Cyber Protect". The card includes a small icon labeled 'A', the product name "Acronis Cyber Protect", a brief description stating it provides backup protection for data, and two buttons: "Truy cập" and "Hướng Dẫn".

- Ta có thể xem thông tin của các công cụ đó



The screenshot shows the "Network Tools" section of the SmartPro website. It features two main items: "Wireshark" and "UltraViewer". Each item has a thumbnail icon, a title, a brief description, and two buttons at the bottom: "Truy cập" (blue) and "Hướng Dẫn" (orange). The "Wireshark" entry includes a note about its capabilities and a link to its documentation.

Wireshark
Wireshark là công cụ phân tích giao thức mạng mạnh mẽ, giúp bắt và phân tích gói tin theo thời gian thực. Nó hỗ trợ nhiều giao thức, cung cấp thông tin...

Truy cập **Hướng Dẫn**

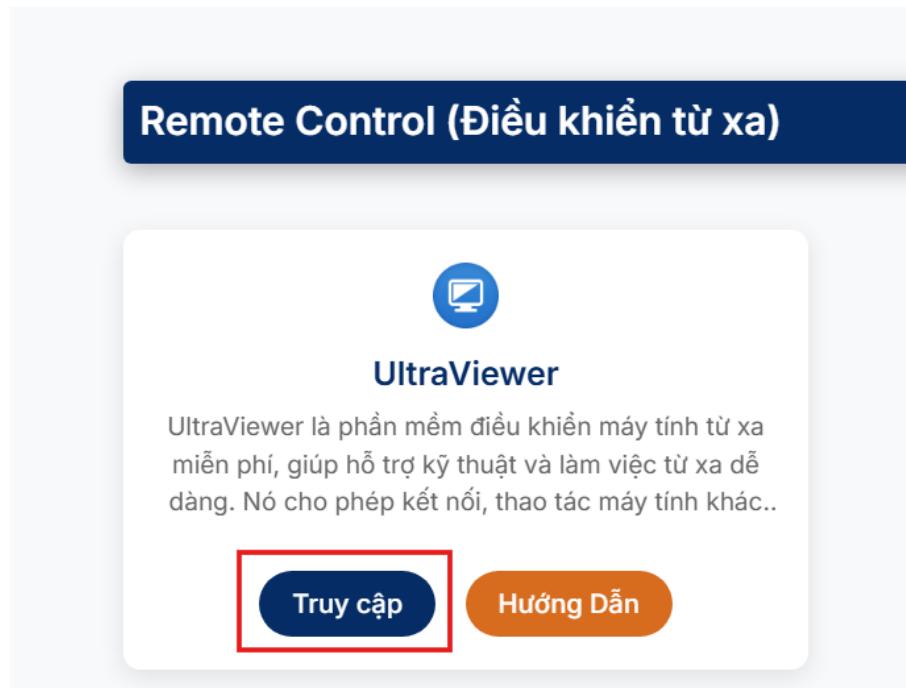
Remote Control (Điều khiển từ xa)

UltraViewer
UltraViewer là phần mềm điều khiển máy tính từ xa miễn phí, giúp hỗ trợ kỹ thuật và làm việc từ xa dễ dàng. Nó cho phép kết nối, thao tác máy tính khác..

Truy cập **Hướng Dẫn**

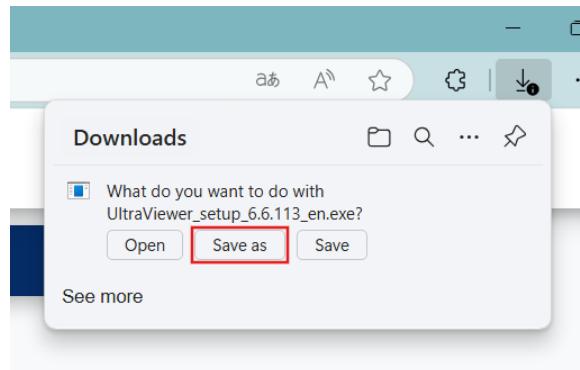
3. Cài đặt UltraViewer

- Ta click vào “Truy Cập” để tải file cài đặt

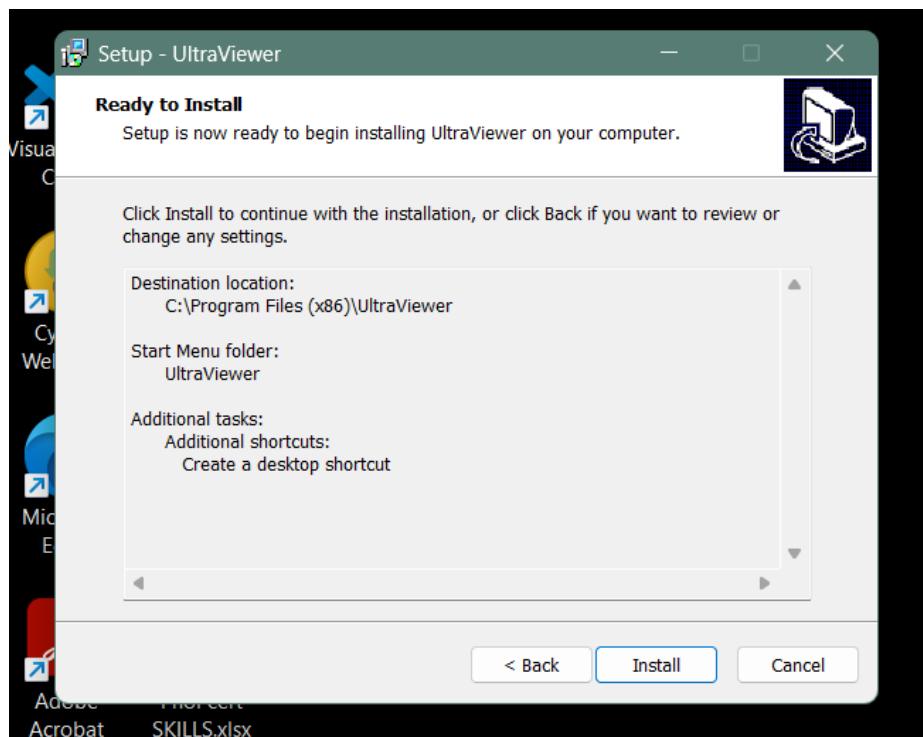


The image shows a zoomed-in view of the "Truy cập" button for the "UltraViewer" entry. The button is highlighted with a red border, and the text "Truy cập" is visible inside it. The background shows the "Remote Control (Điều khiển từ xa)" section of the website.

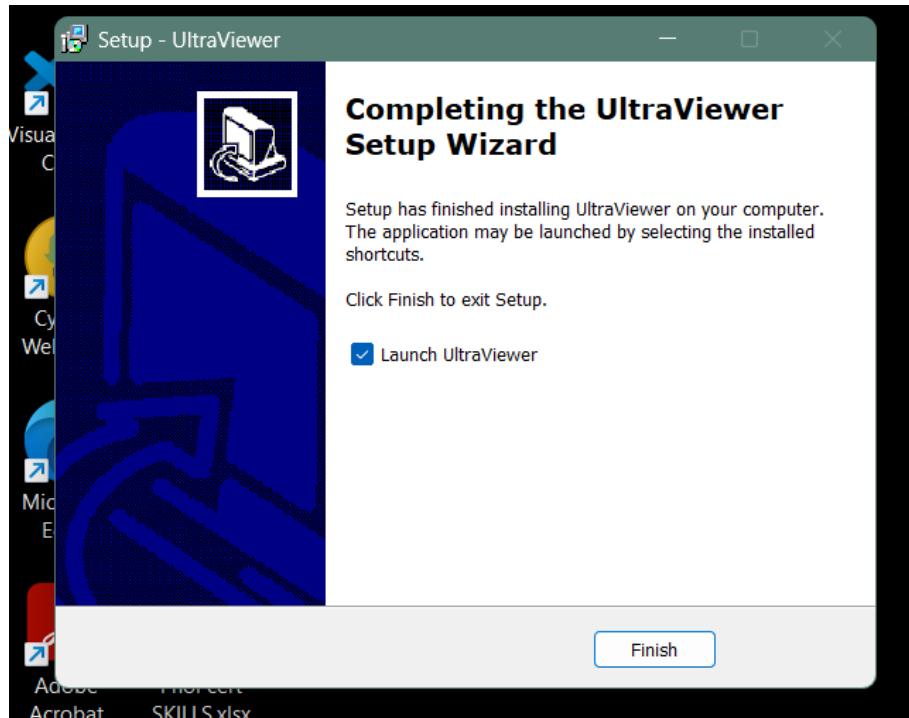
- Sau khi popup trình tải về, ta chọn “save as” để chọn nơi lưu trữ



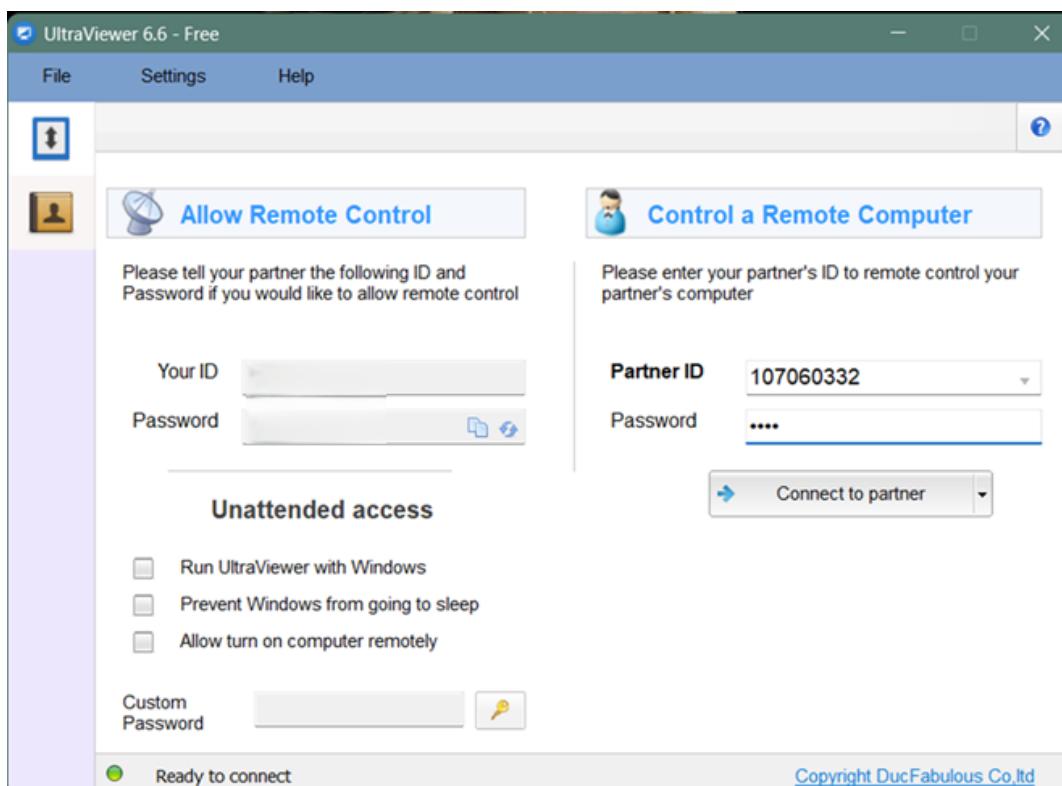
- Ta chọn “Install” để bắt đầu cài đặt.



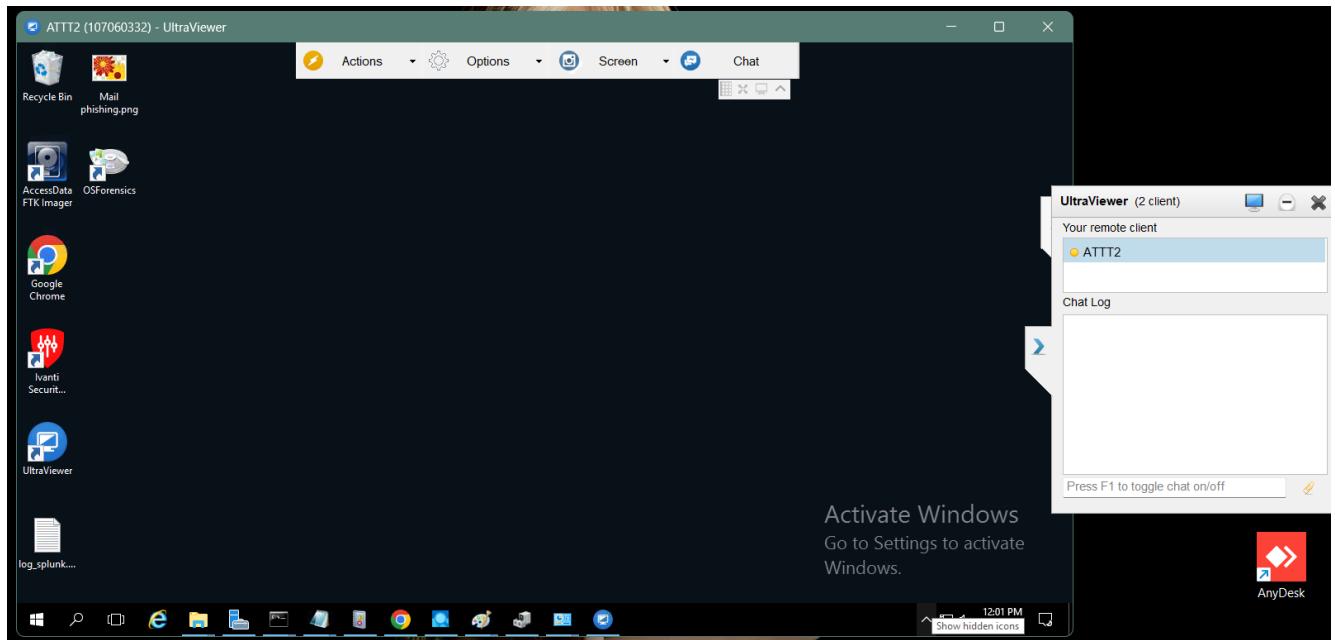
- Ở các bước tiếp theo, ta chỉ cần bấm “Next” cho đến khi trình cài đặt được hoàn tất và nhấn “Finish” để chạy ứng dụng



- Sau khi cài đặt thành công sẽ có giao diện như bên dưới. Ta chỉ cần nhập vào “Partner ID” và “Password” và nhấn vào “Connect to partner” để tiến hành remote từ xa

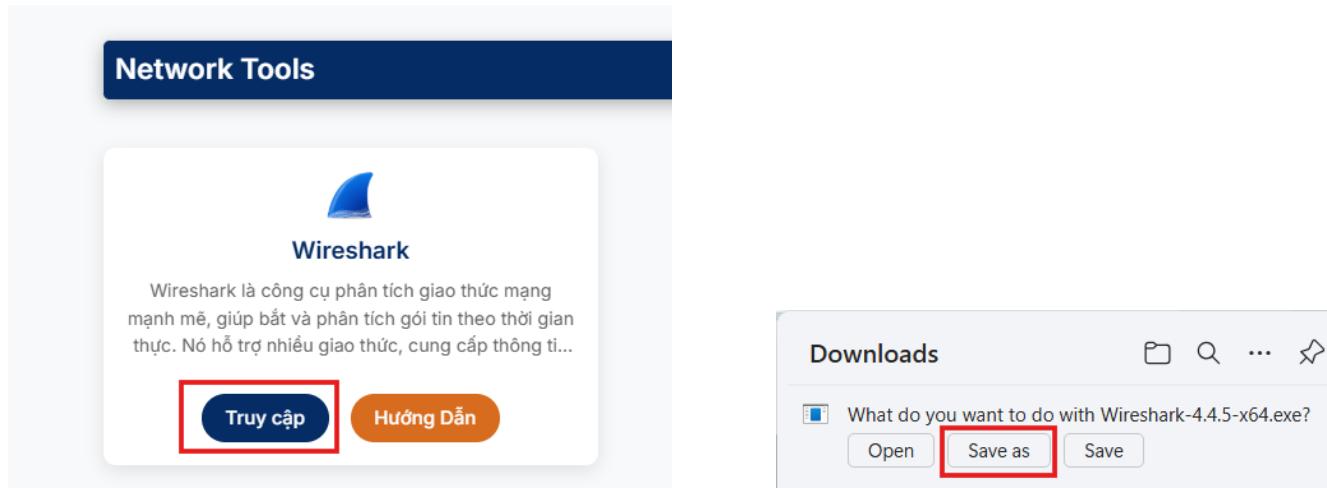


- Sau khi remote thành công tiến hành các công việc diển tập

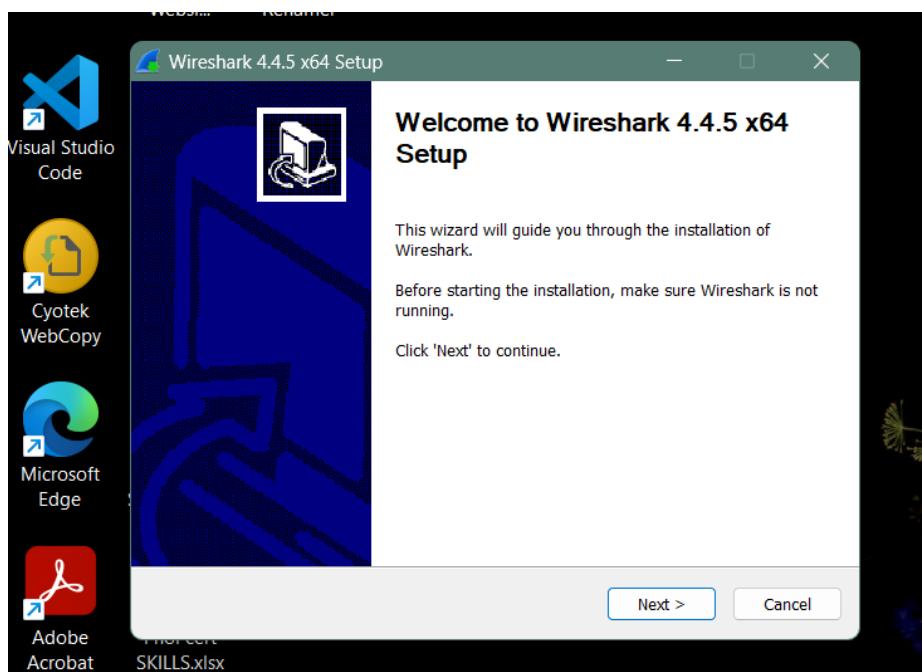


4. Cài Đặt Wireshark

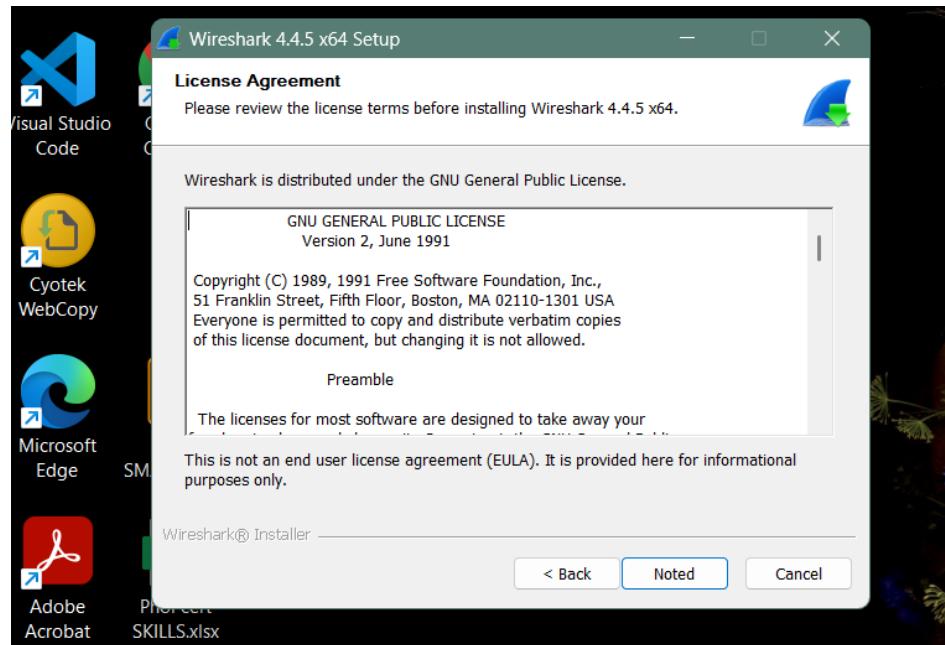
- Ta chọn “Truy Cập” để hệ thống tự động popup trình tải về và chọn “Save As” để chọn nơi lưu trữ



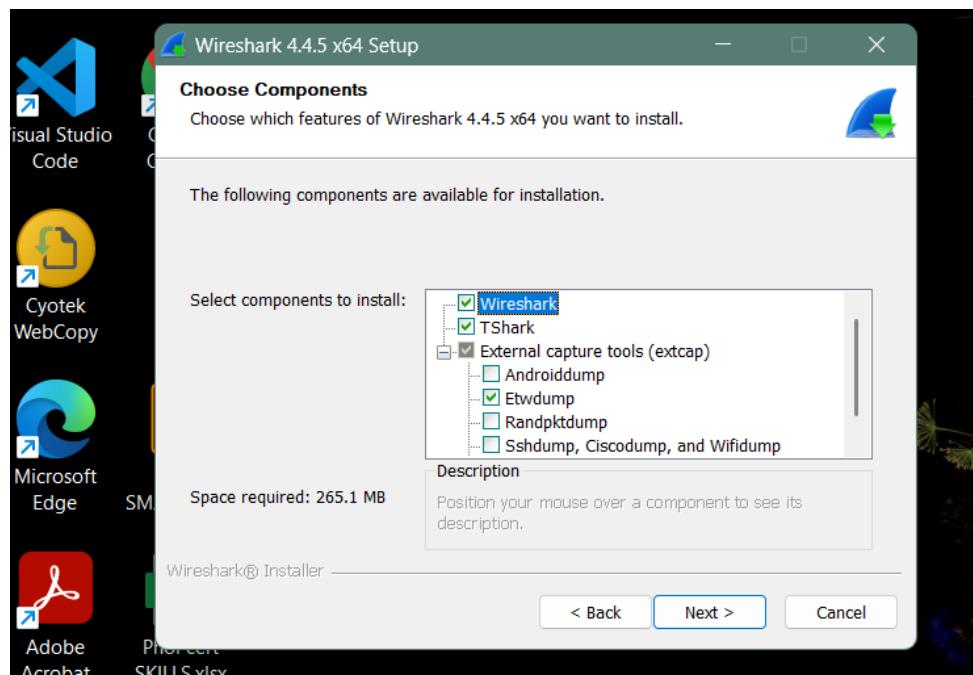
- Ta chọn Next



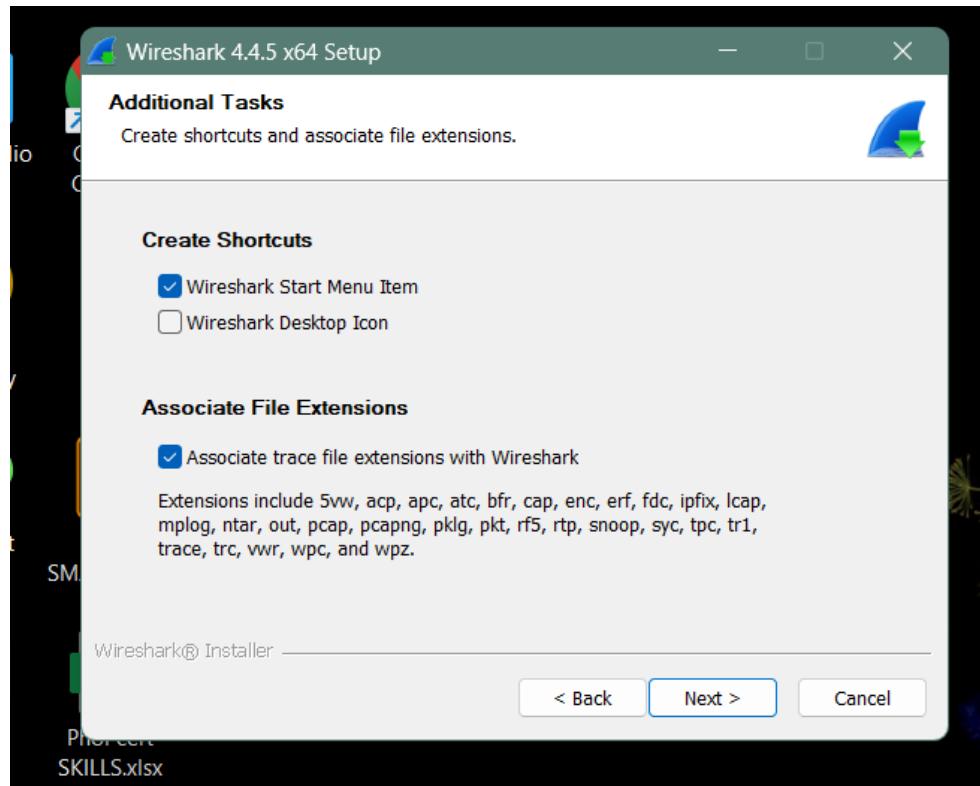
- Ta chọn “Noted”



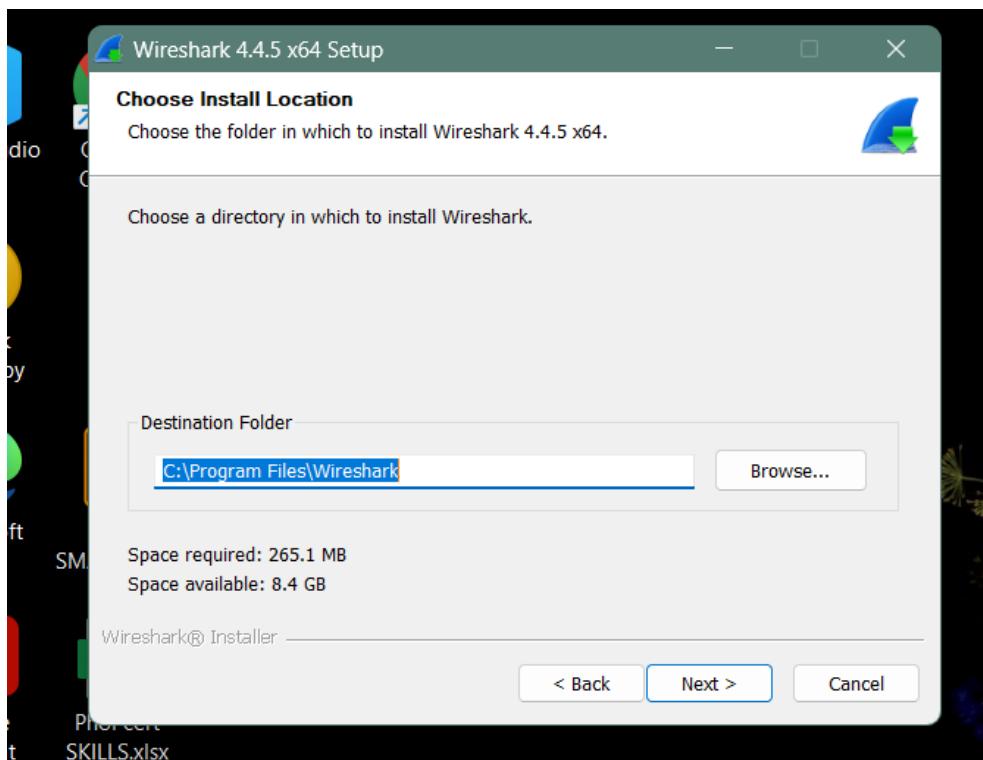
- Ta chọn “Next”



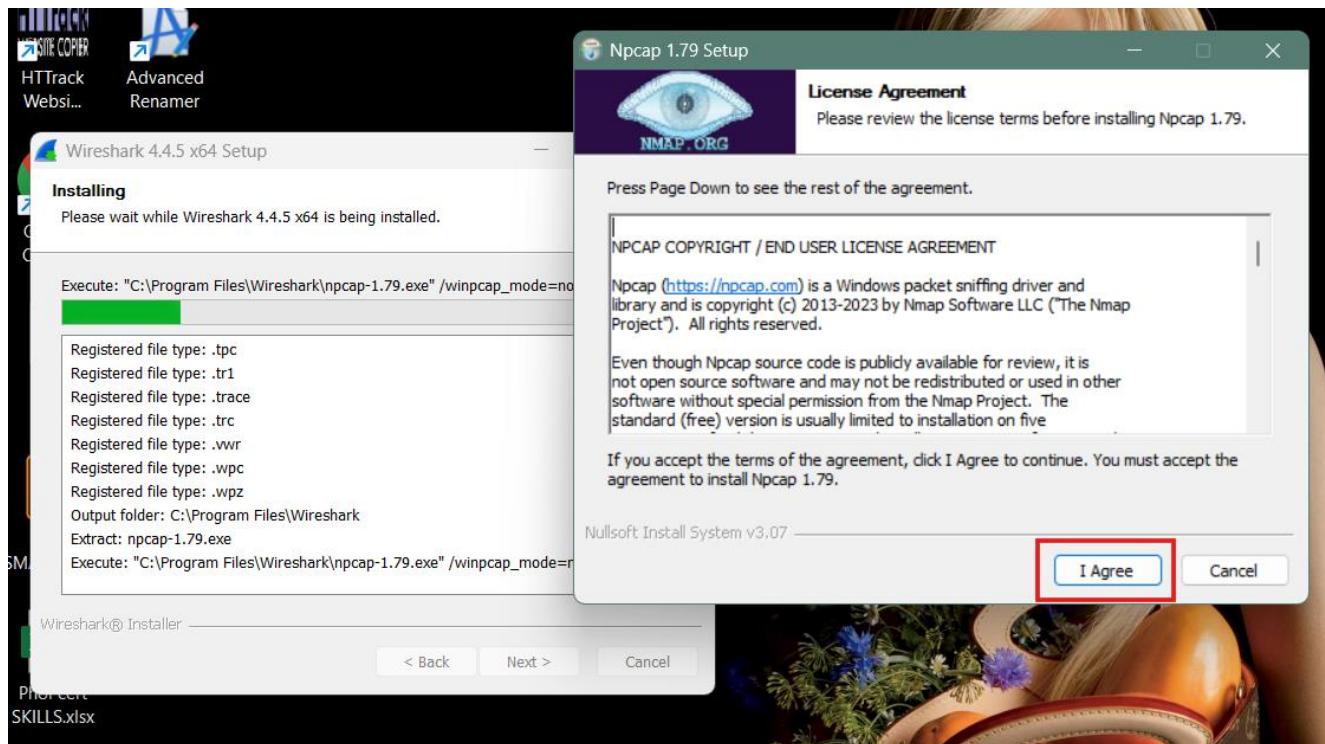
- Ta chọn “Next”



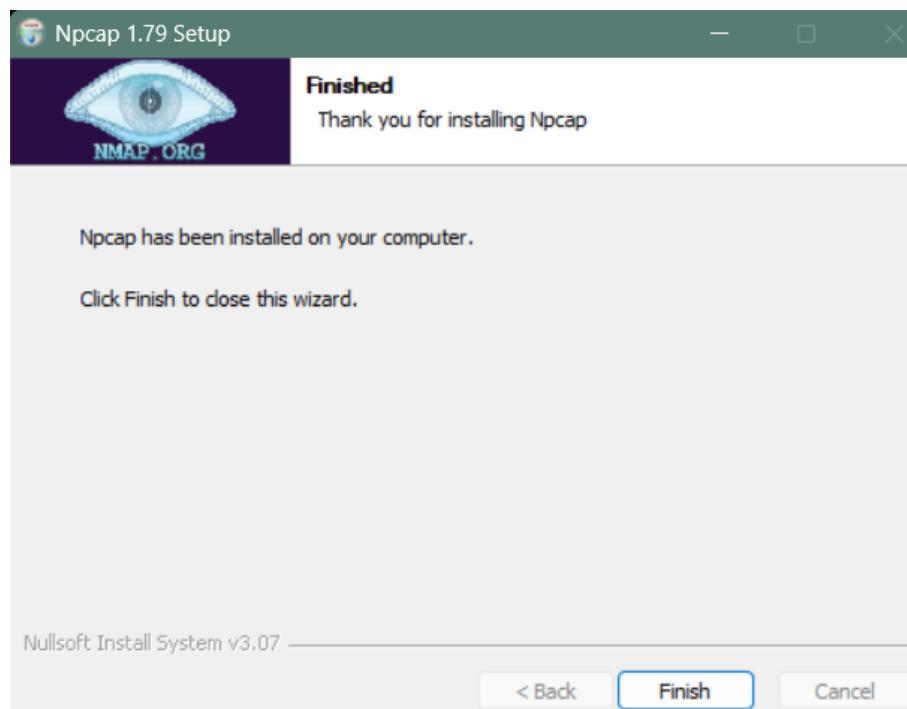
- Chọn “Next” để chọn nơi lưu trữ



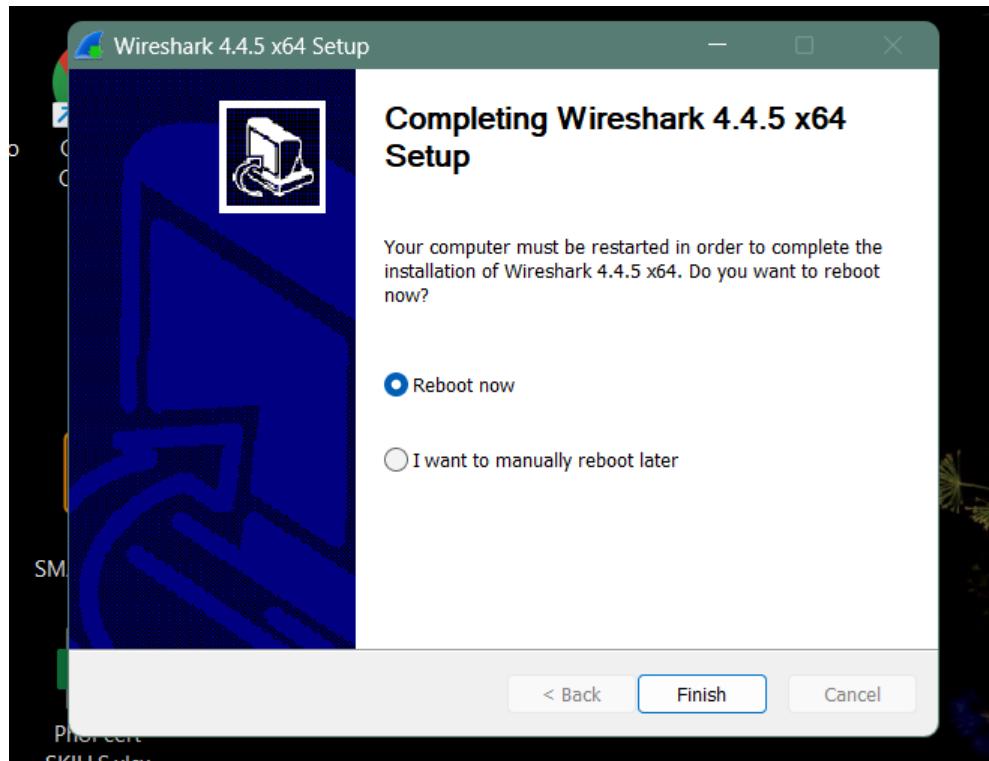
- Chọn “I Agree”



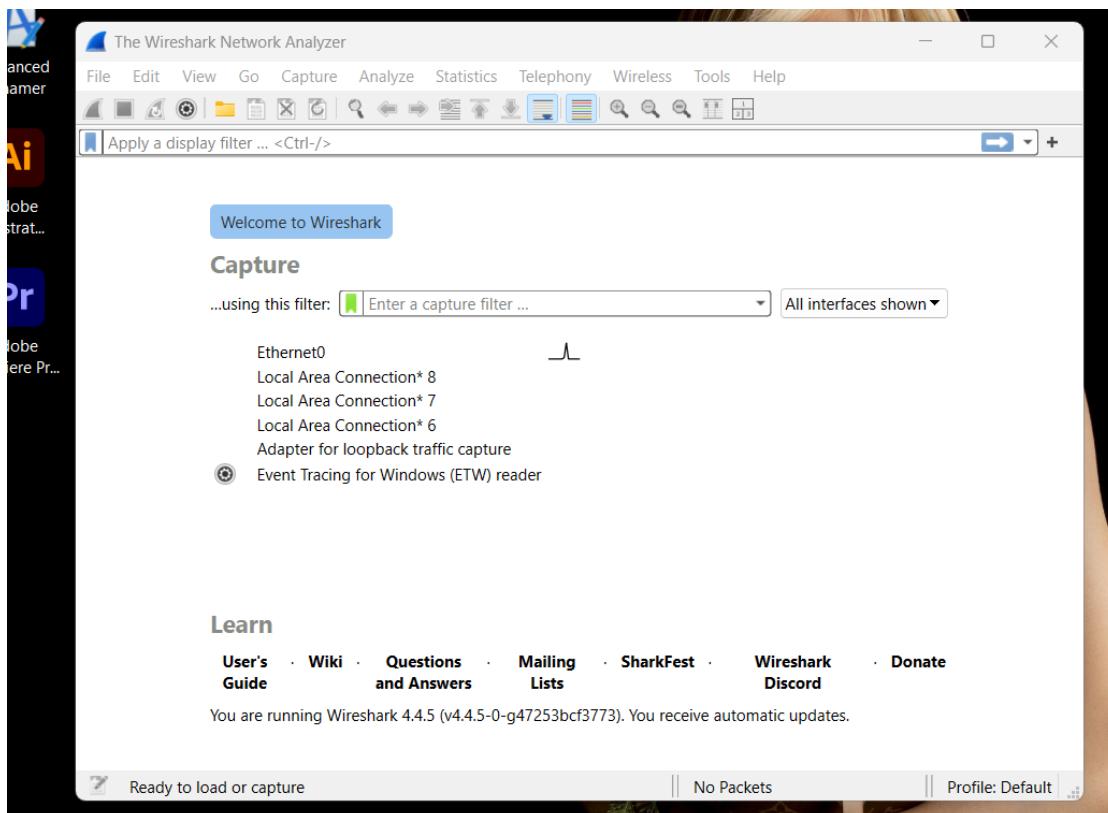
- Chọn “Finish”



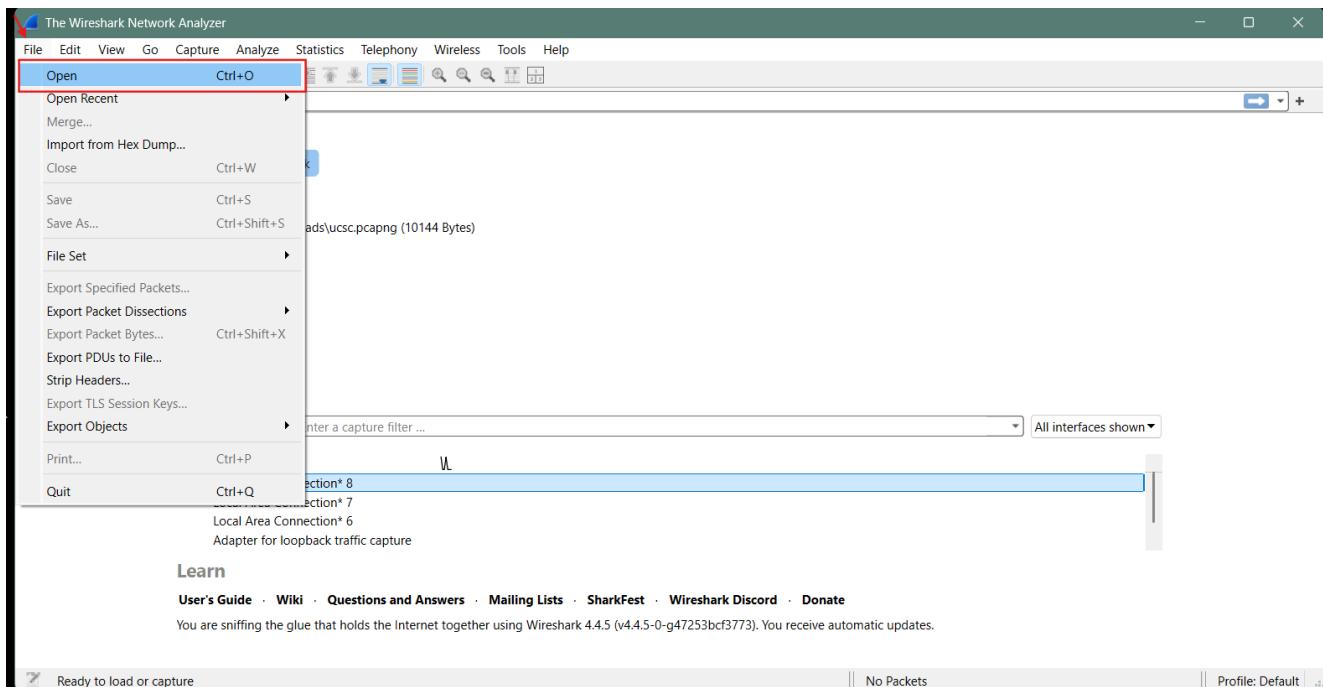
- Chọn “Finish”



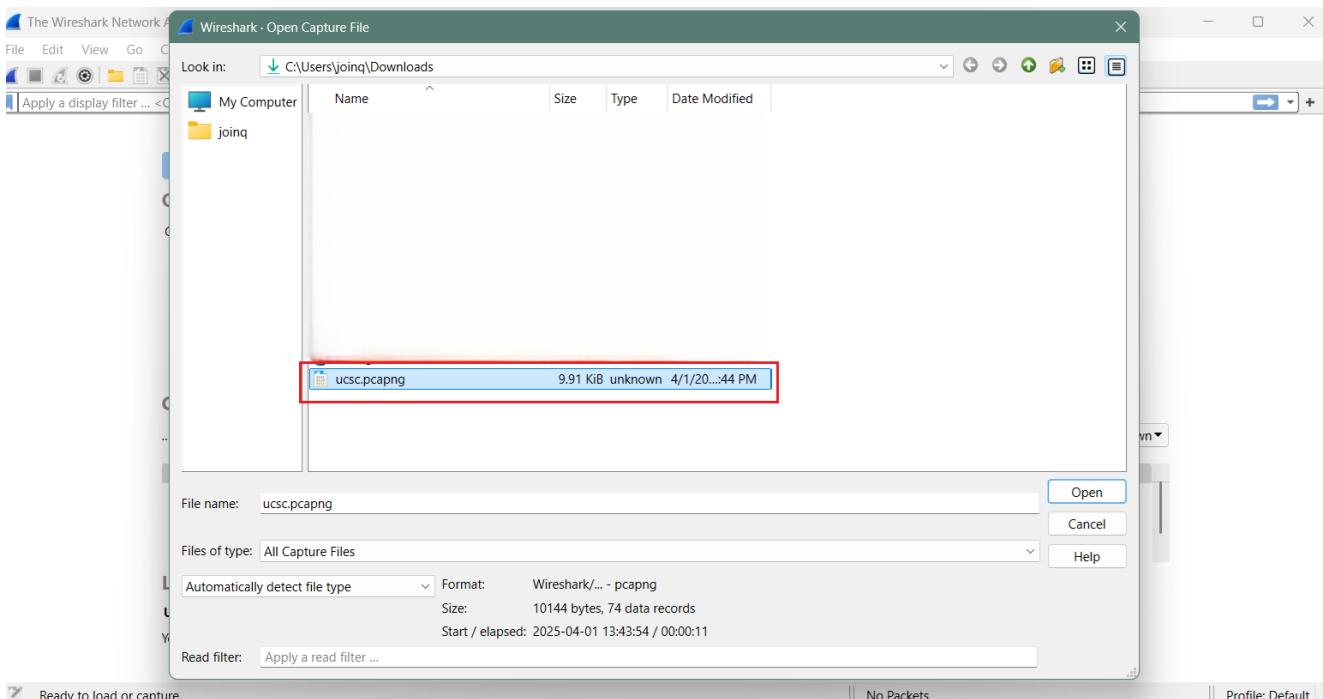
- WireShark sẽ có giao diện như sau



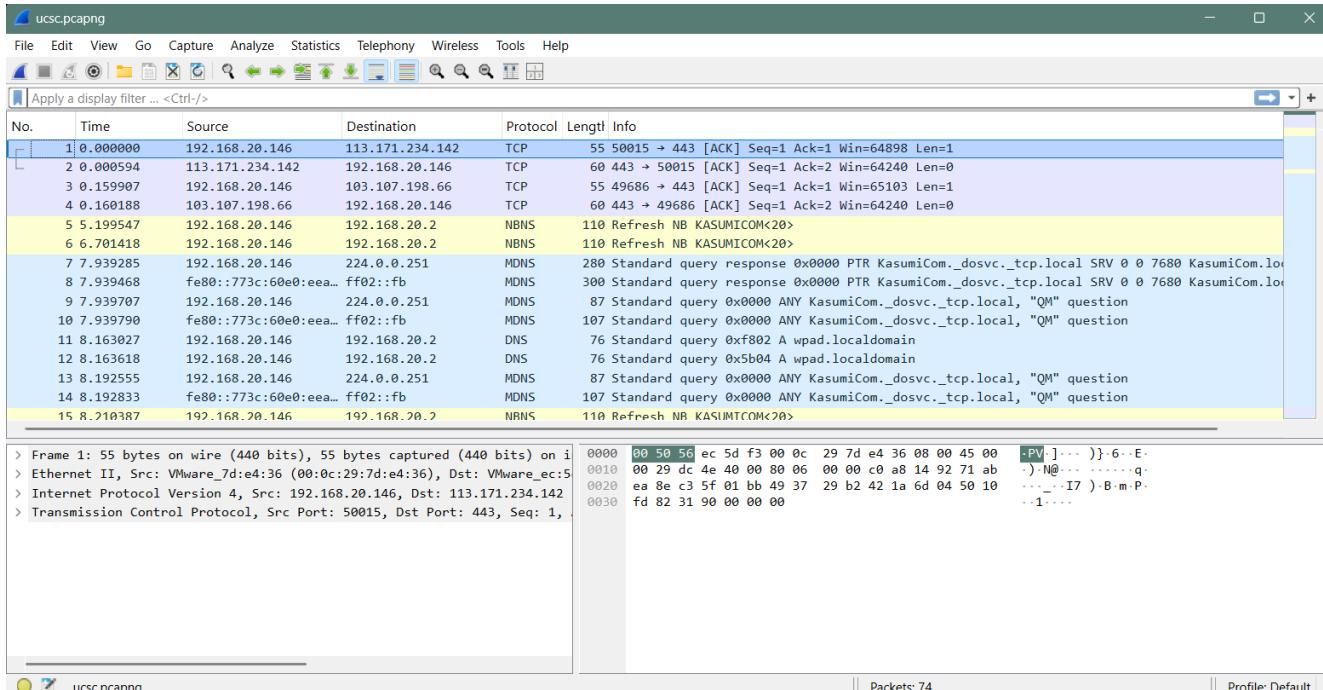
- Ta chọn “File” → “Open” để mở file



- Ta chọn nơi lưu trữ file “ucsc.pcapng” và bấm “Open”



- Sau Khi đã open thành công, ta sẽ thấy giao diện như bên dưới

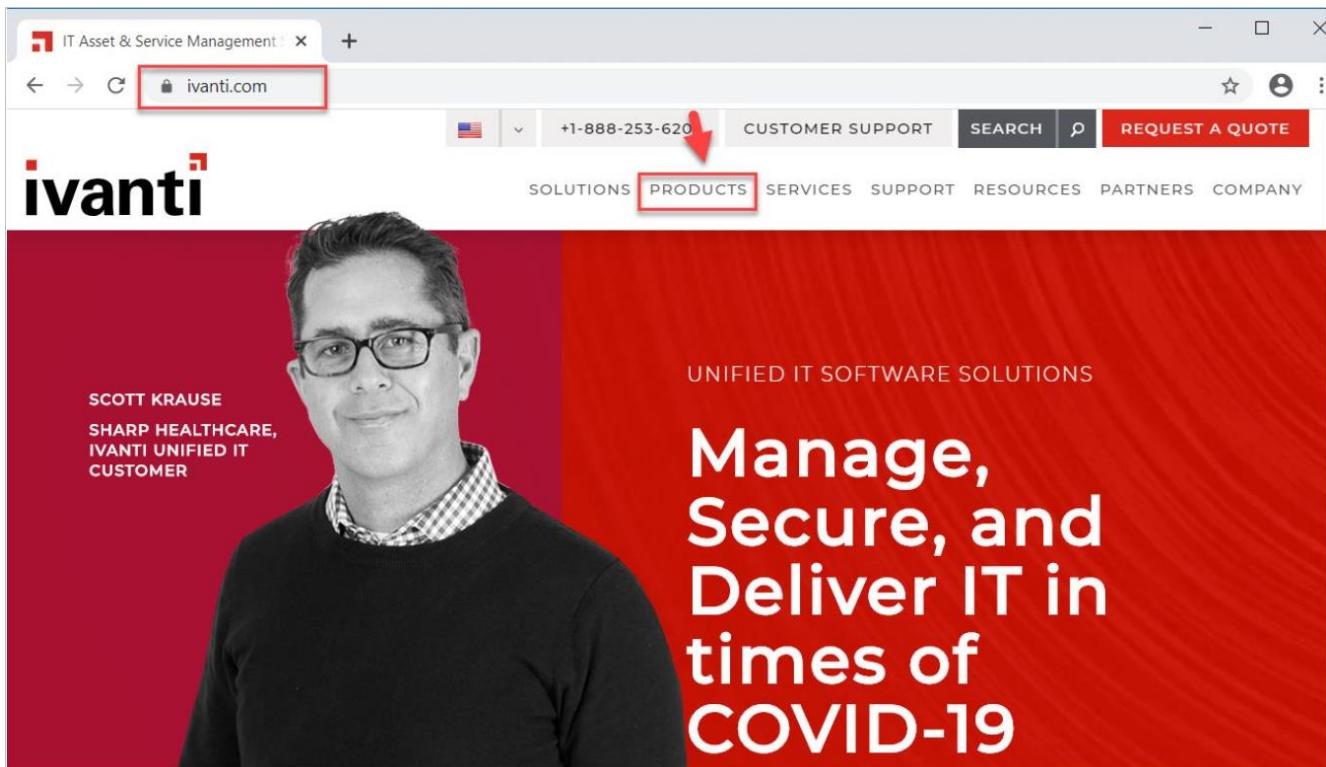


5. Ivanti Security Controls

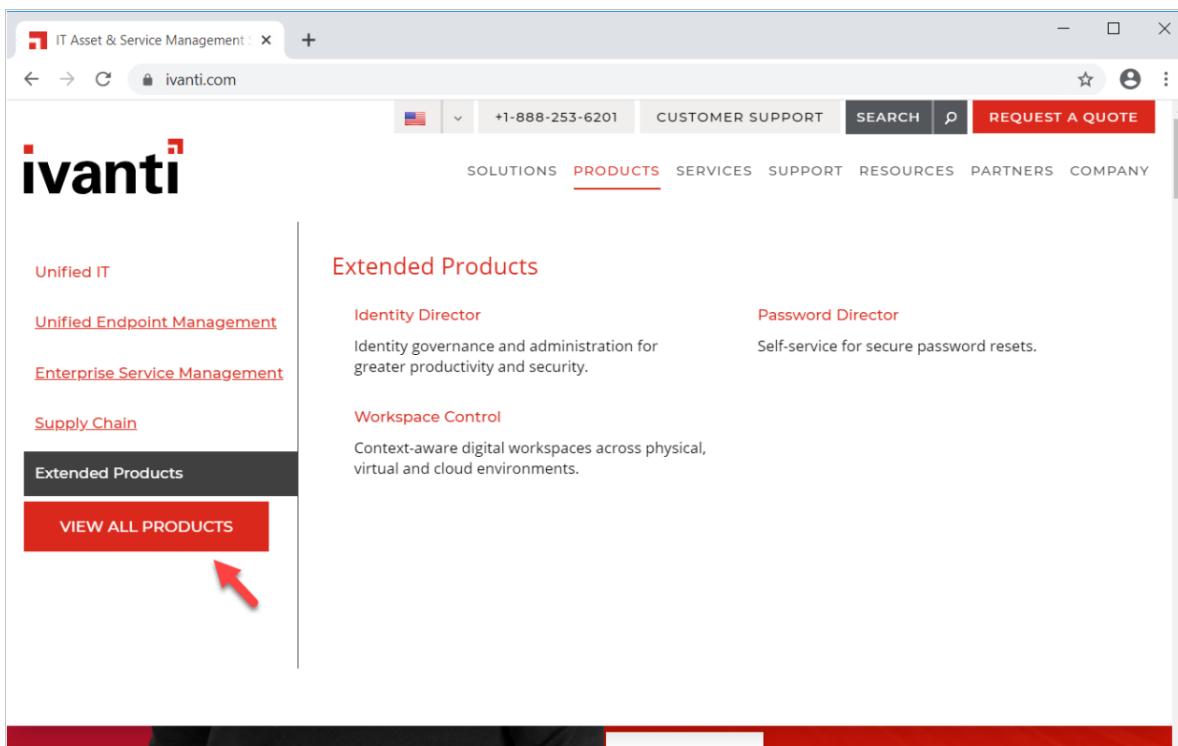
- **Phần 1: Giới thiệu về Ivanti Security Controls**
 - **Ivanti Security Controls (ISeC)** là công cụ hỗ trợ:
 - Rà quét các lỗ hổng phổ biến (CVE) và lỗ hổng Zero-Day trên hệ thống máy chủ.
 - Cung cấp các bản vá để khắc phục nhanh chóng.
 - **Ưu điểm nổi bật:**
 - Hỗ trợ rà quét hệ thống máy chủ Windows bằng cơ chế Agentless (không cần cài đặt agent trên máy mục tiêu).
 - Kết quả rà quét chính xác, với khả năng phát hiện dấu hiệu lỗ hổng trong 60 ngày và hỗ trợ tối đa 50 node mạng mà không giới hạn tính năng.
- **Phần 2: Chuẩn bị môi trường cài đặt và Yêu cầu tài nguyên**
 - **Tải xuống:** Truy cập liên kết: https://forums.ivanti.com/s/article/IvantiSecurity-Controls-Download?language=en_US
 - **Cấu hình máy ảo (VM):**
 - CPU: Tối thiểu 8 nhân.
 - RAM: 16 GB.
 - Ổ cứng: SSD 250 GB.
 - Hệ điều hành: Windows Server 2019 hoặc phiên bản mới hơn.
 - Yêu cầu kết nối Internet để cập nhật dấu hiệu nhận dạng lỗ hổng và bản vá.
- **Phần 3: Cài đặt Ivanti Security Controls**

Dưới đây là các bước chi tiết để cài đặt ISeC:

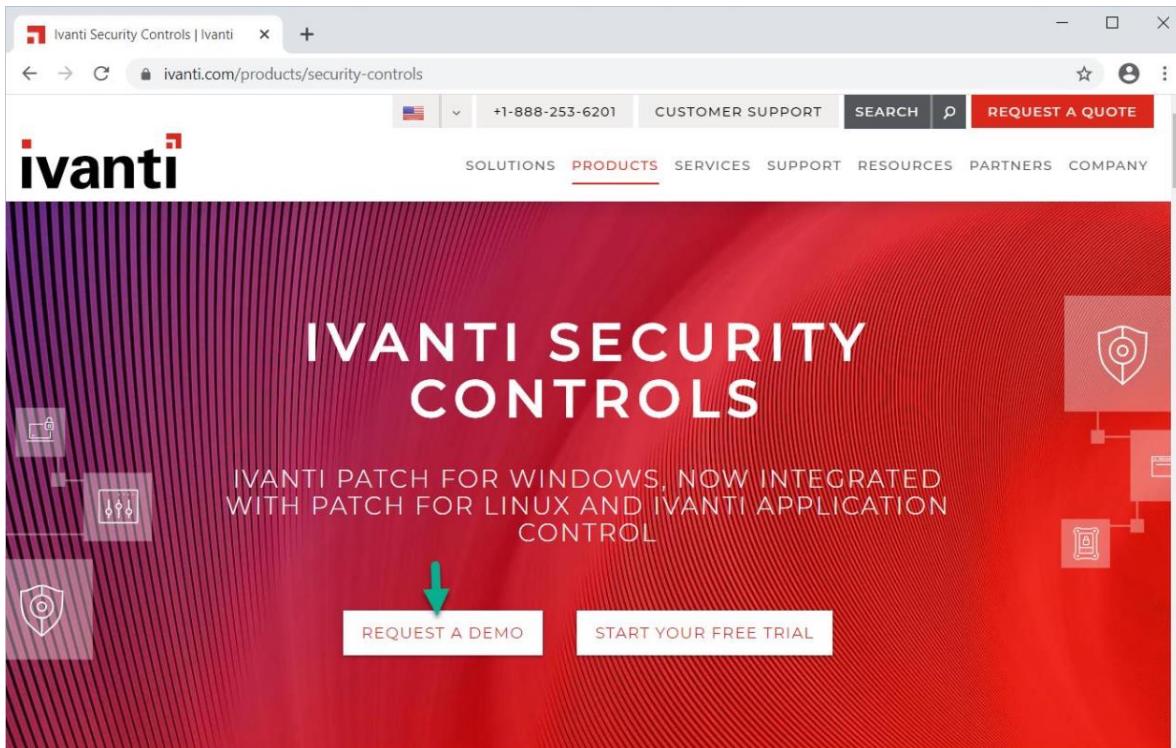
 - **Tải phần mềm:**
 - Truy cập ivanti.com.
 - Chọn **PRODUCTS**.



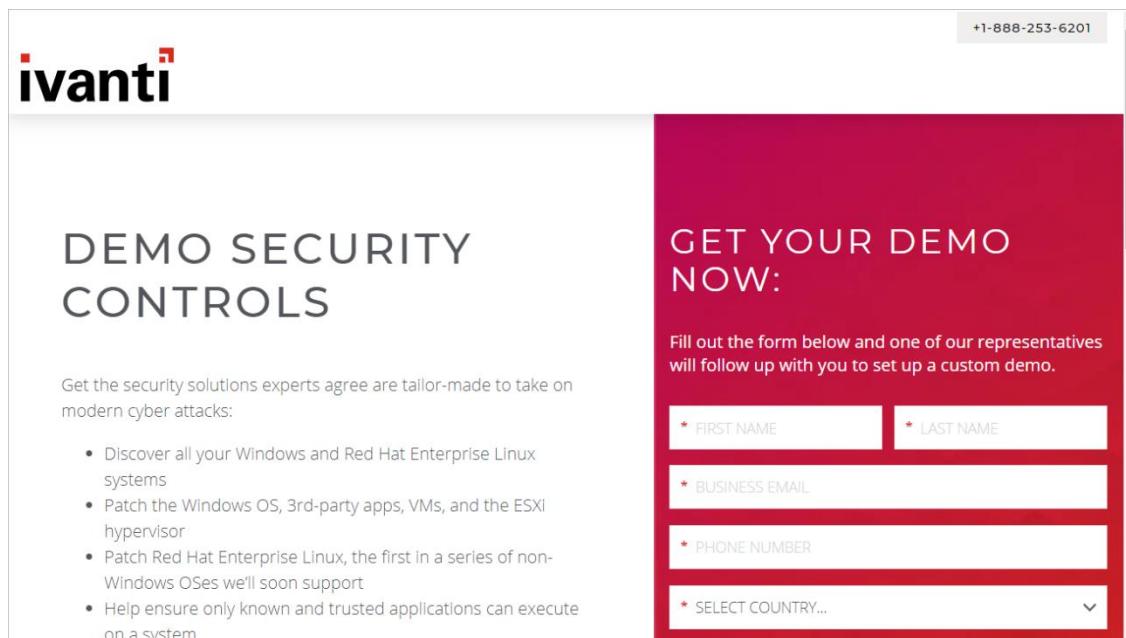
○ Nhập vào **VIEW ALL PRODUCTS**.



- Tìm **Ivanti Security Controls** và chọn **REQUEST A DEMO**.

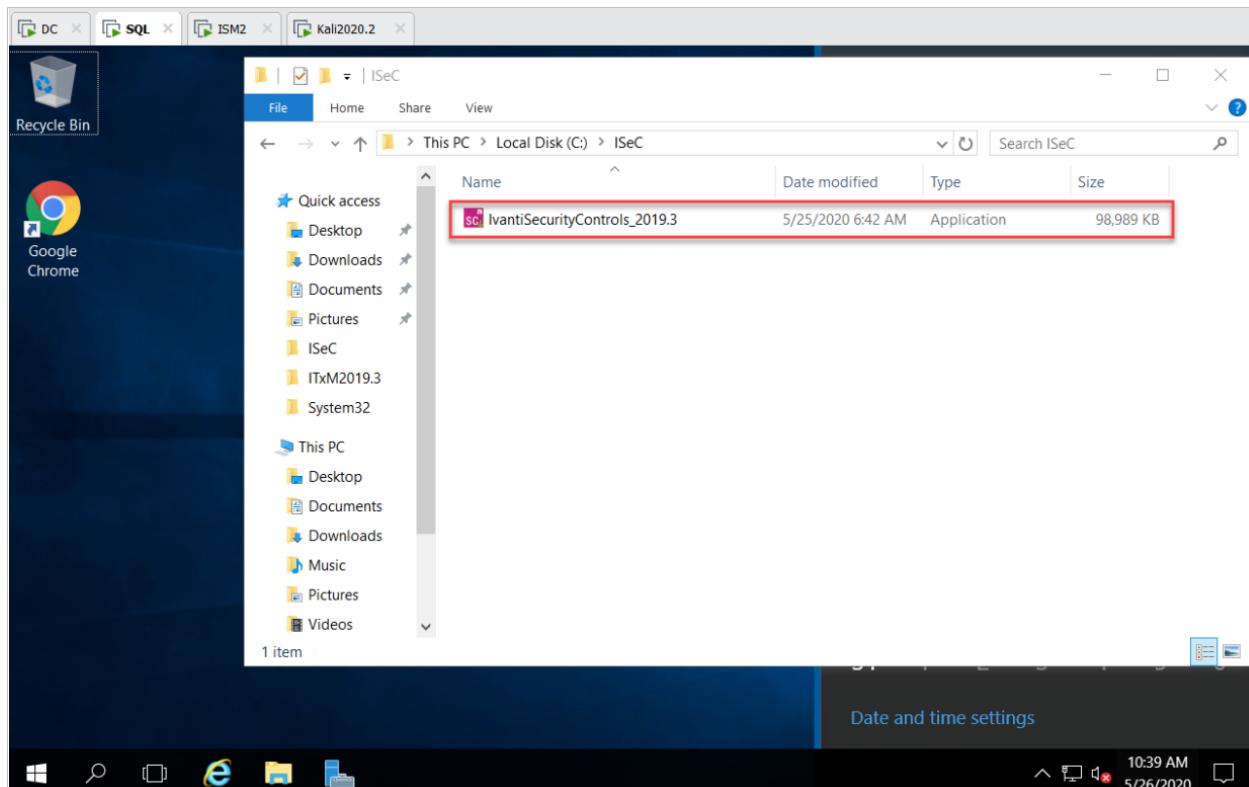


- Điền thông tin cá nhân để nhận liên kết tải xuống.



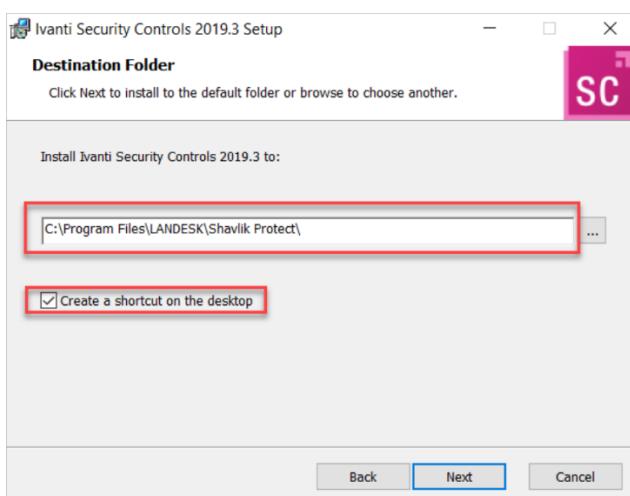
Chuẩn bị cài đặt:

- Sao chép tệp cài đặt vào máy ảo chạy Windows Server 2016 hoặc phiên bản mới hơn.



Bắt đầu cài đặt:

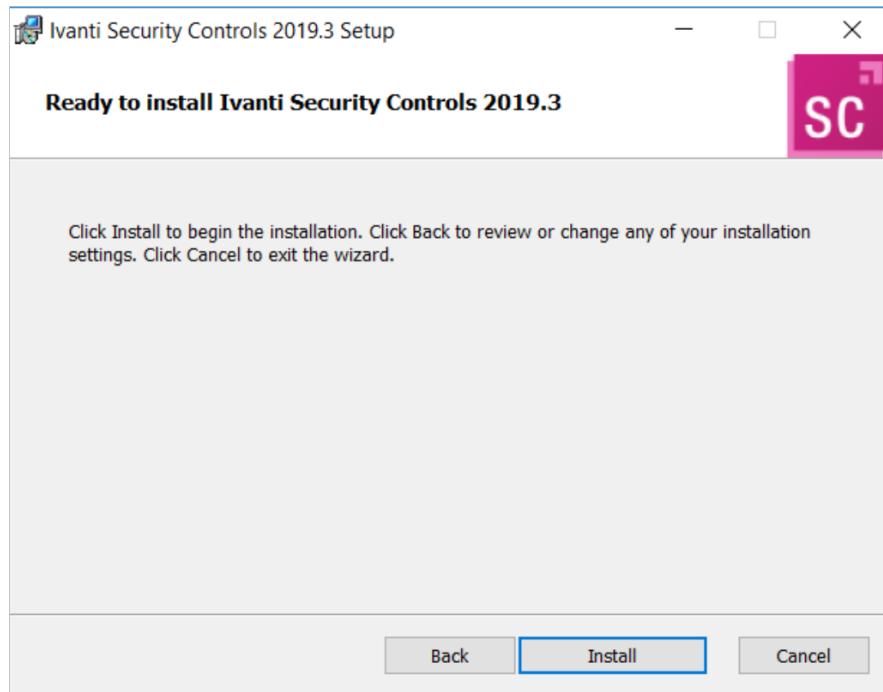
- Mở tệp cài đặt Ivanti Security Controls 2019.3 Setup.



- Chọn Next tại màn hình Destination Folder (thư mục mặc định: C:\Program Files\LANDESK\Shavlik Protect).

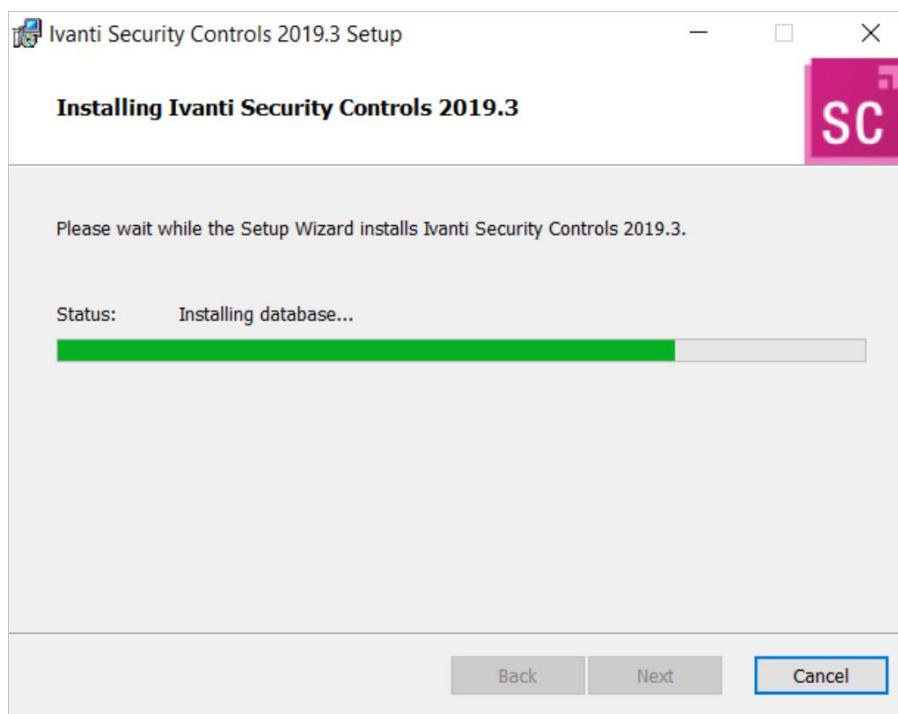
Xác nhận cài đặt:

- Tại màn hình **Ready to Install**, nhấp **Install** để bắt đầu quá trình cài đặt.



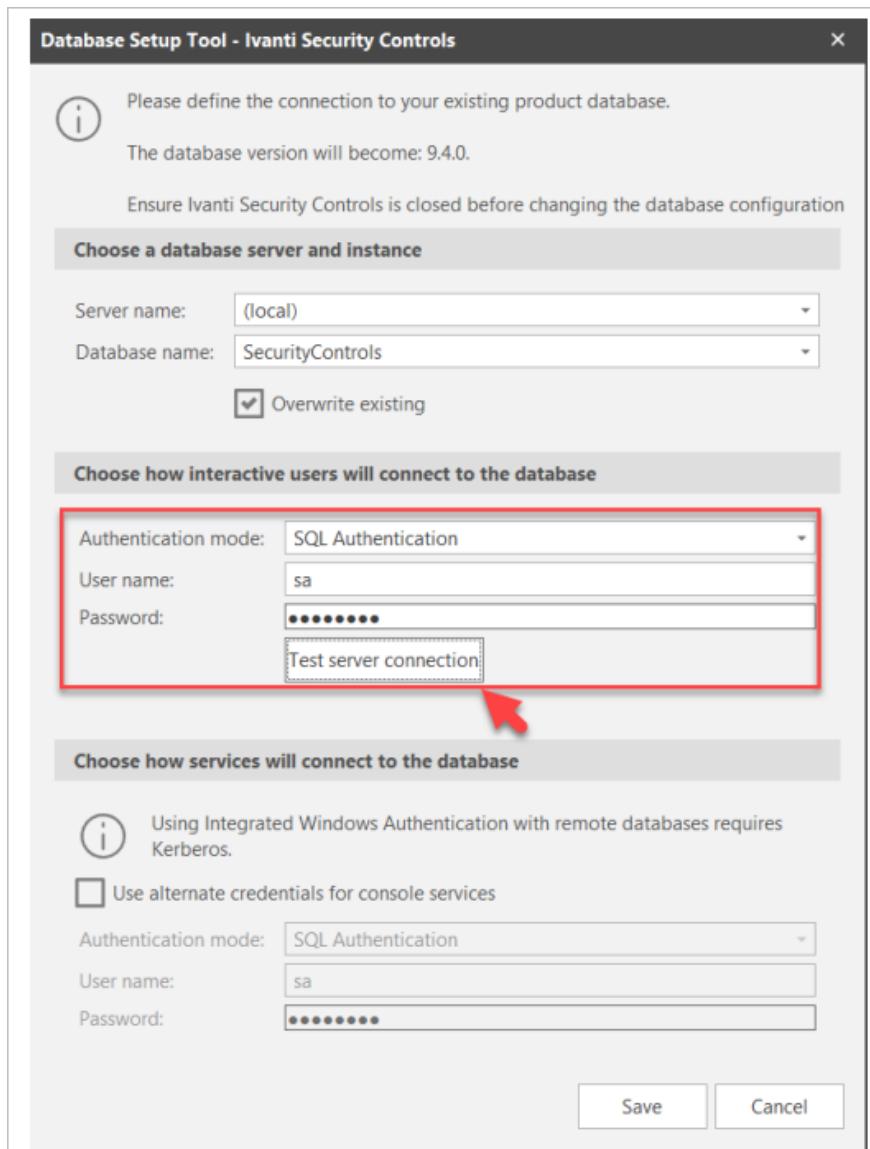
Chờ cài đặt hoàn tất:

- Quá trình cài đặt sẽ hiển thị trạng thái, ví dụ: "Installing database...".



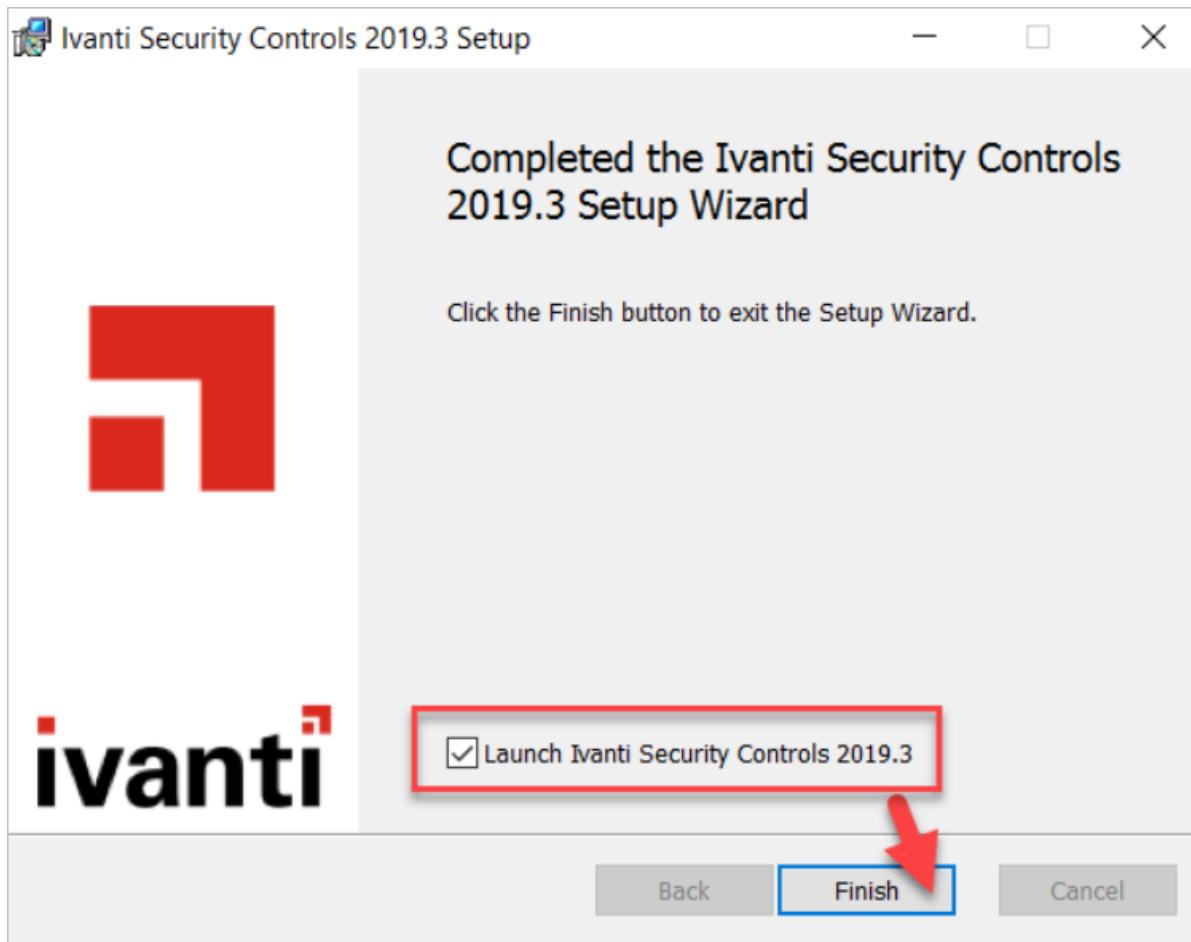
Cấu hình cơ sở dữ liệu:

- Sau khi cài đặt, mở **Database Setup Tool**.
- Nhập thông tin:
 - **Server name:** (local) (hoặc tên server của bạn).
 - **Database name:** SecurityControls.
 - **Authentication mode:** SQL Authentication.
 - **User name:** sa (hoặc tài khoản SQL của bạn).
 - **Password:** Nhập mật khẩu tương ứng.
- Nhấn **Test server connection** để kiểm tra kết nối, sau đó nhấn **Save**.



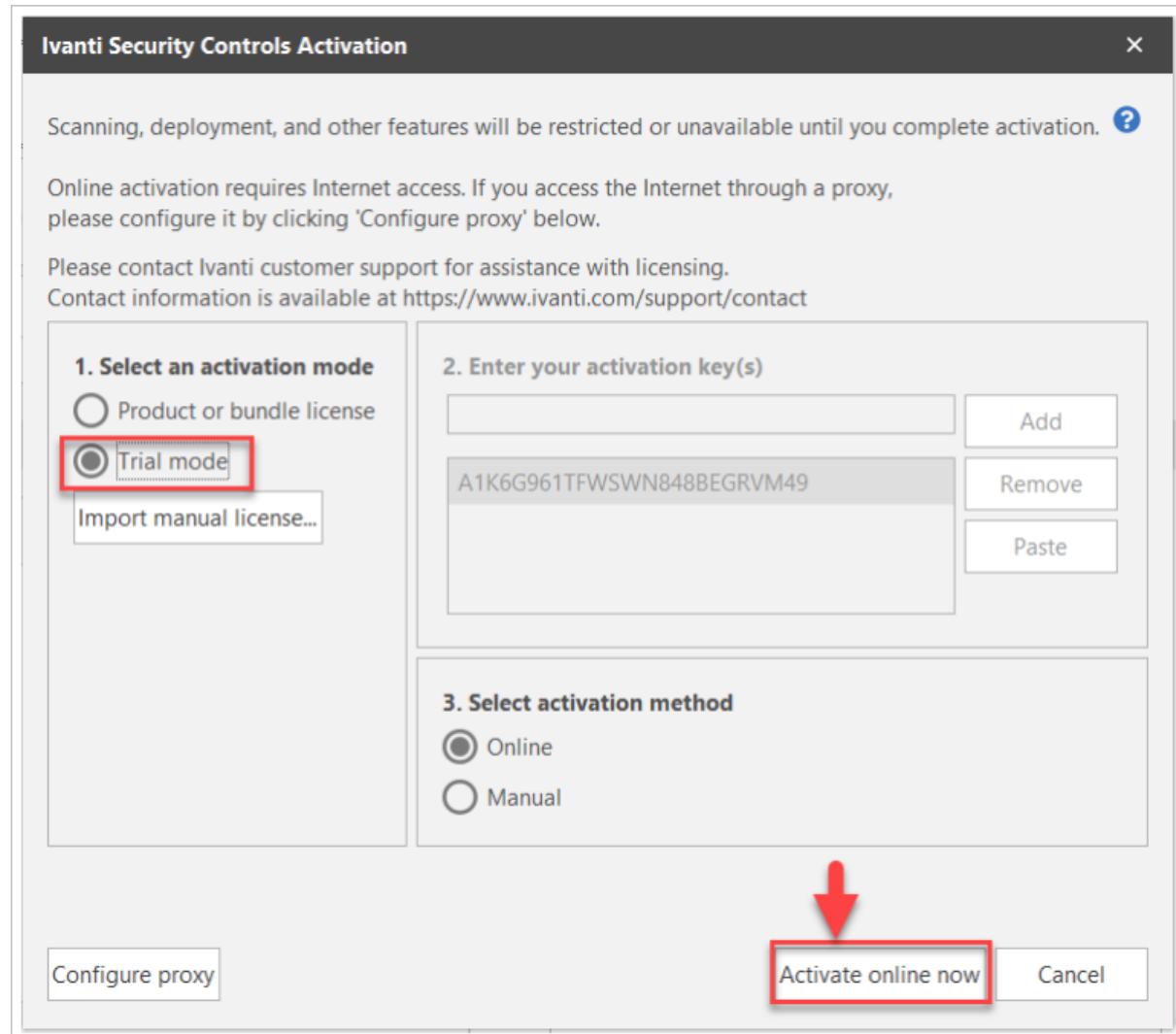
Hoàn tất cài đặt:

- Tại màn hình Completed the Ivanti Security Controls 2019.3 Setup Wizard, chọn **Launch Ivanti Security Controls 2019.3**, rồi nhấn **Finish**.



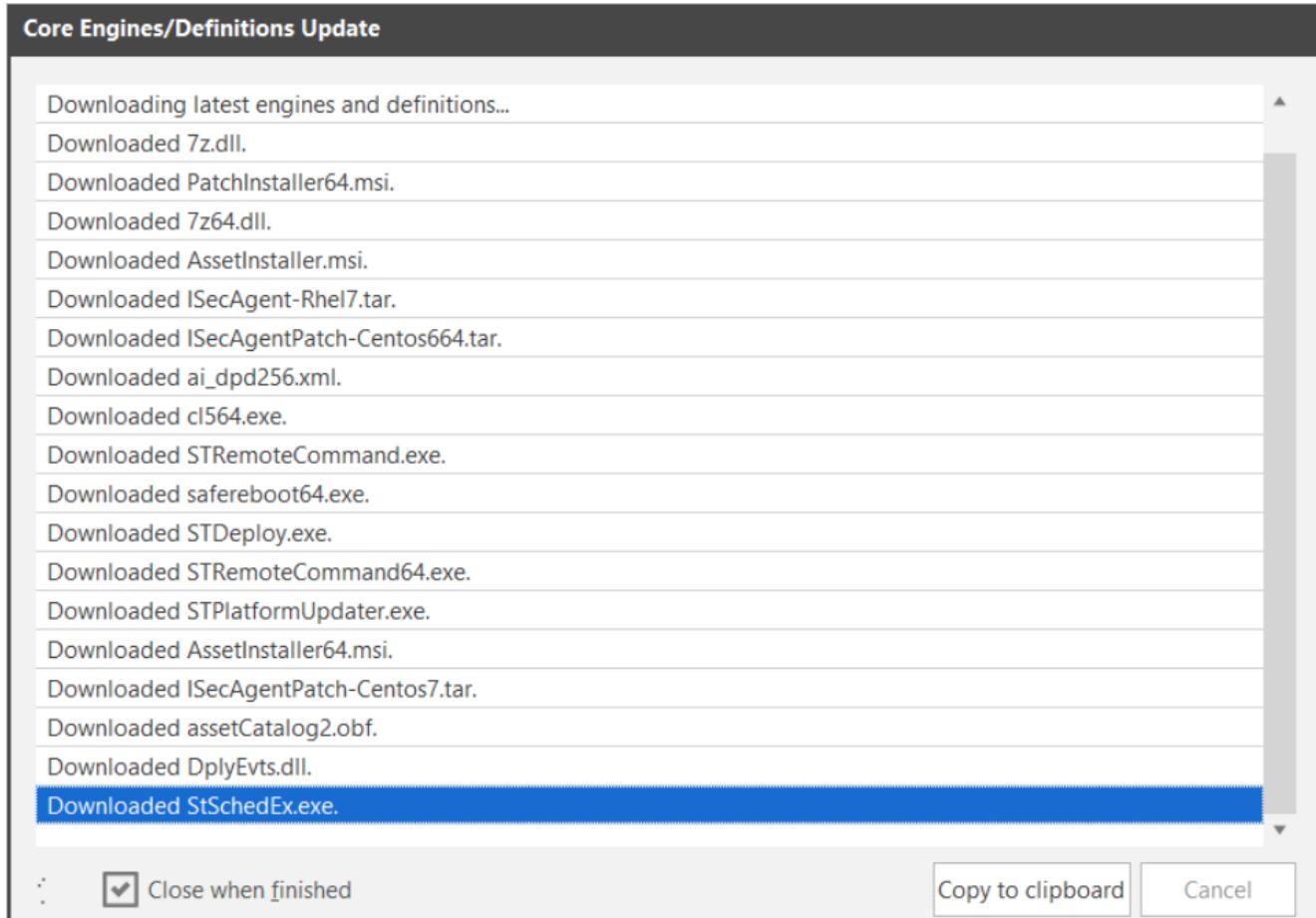
Kích hoạt phần mềm:

- Khi khởi động ISeC lần đầu, chọn:
 - **Trial mode** (chế độ dùng thử).
 - **Activate online now** (kích hoạt trực tuyến, yêu cầu kết nối Internet).



Tải xuống định nghĩa lỗ hổng:

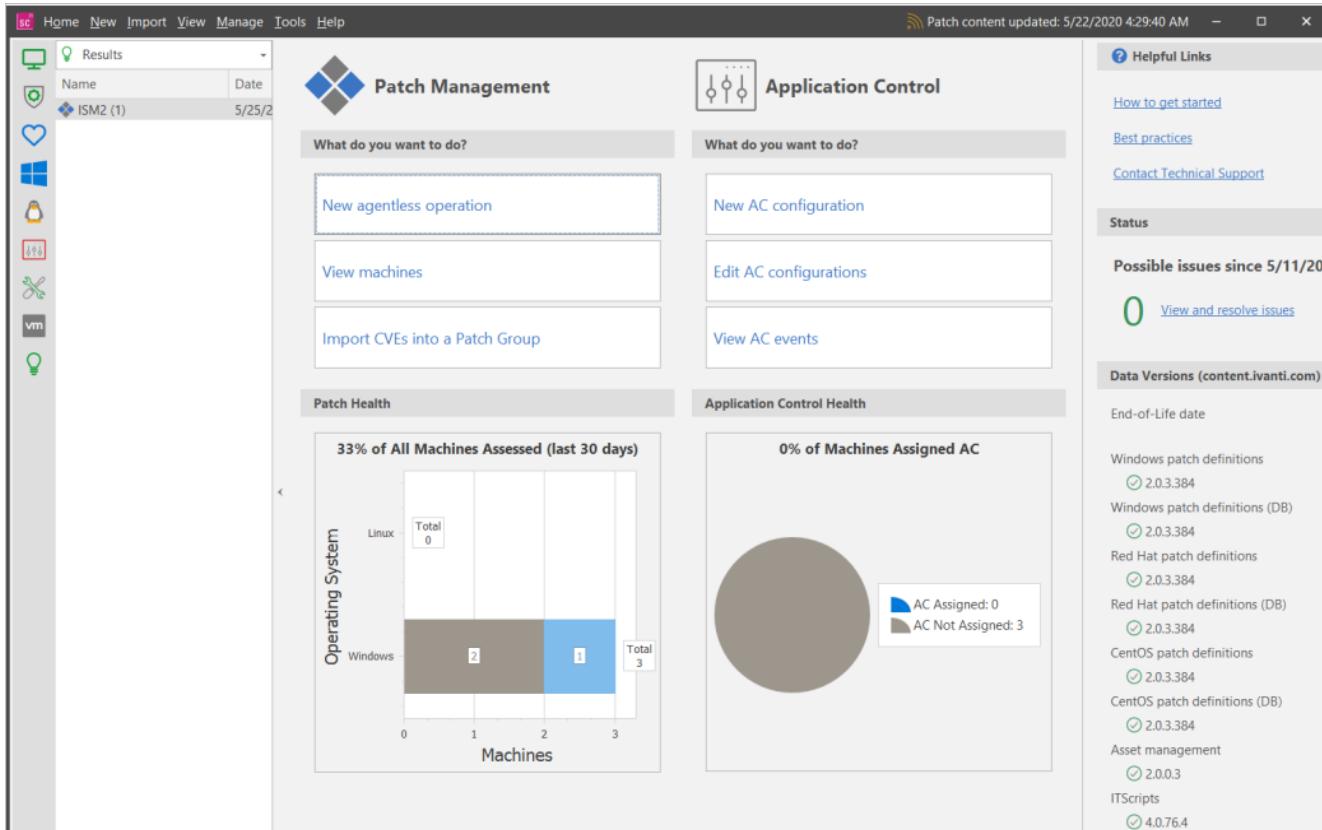
- Chờ hệ thống tải các tệp định nghĩa (definitions) như 7z.dll,
PatchInstaller64.msi, v.v.



- Nhấn **Close when finished** khi hoàn tất.

Mở giao diện ISeC:

- Sau khi cài đặt và kích hoạt, giao diện chính của ISeC sẽ hiện ra (ví dụ: tab **Patch**).



The screenshot shows the ISeC Patch Management interface. On the left, there's a sidebar with various icons: Home, New, Import, View, Manage, Tools, Help, Results, Name (ISM2 (1)), Date (5/25/2), and a lightbulb icon. The main area has two main sections: "Patch Management" and "Application Control".

Patch Management:

- What do you want to do?**
 - New agentless operation
 - View machines
 - Import CVEs into a Patch Group
- Patch Health**: A chart titled "33% of All Machines Assessed (last 30 days)" showing machine counts for Linux and Windows. The chart indicates 0 Linux machines and 3 Windows machines (2 AC Not Assigned, 1 AC Assigned). The legend shows a blue square for "AC Assigned: 0" and a grey square for "AC Not Assigned: 3".

Application Control:

- What do you want to do?**
 - New AC configuration
 - Edit AC configurations
 - View AC events
- Application Control Health**: A chart titled "0% of Machines Assigned AC" showing 0% of machines assigned AC. The legend shows a blue square for "AC Assigned: 0" and a grey square for "AC Not Assigned: 3".

Right Sidebar:

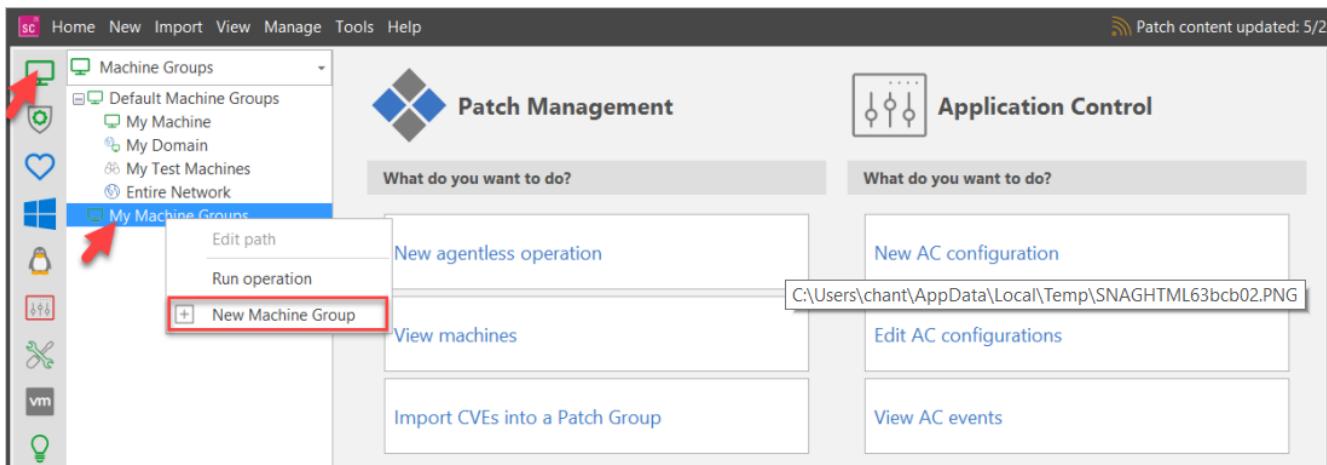
- Helpful Links**: How to get started, Best practices, Contact Technical Support.
- Status**: Possible issues since 5/11/20, 0 View and resolve issues.
- Data Versions (content.ivanti.com)**:
 - End-of-Life date
 - Windows patch definitions: 2.0.3.384 (green checkmark)
 - Windows patch definitions (DB): 2.0.3.384 (green checkmark)
 - Red Hat patch definitions: 2.0.3.384 (green checkmark)
 - Red Hat patch definitions (DB): 2.0.3.384 (green checkmark)
 - CentOS patch definitions: 2.0.3.384 (green checkmark)
 - CentOS patch definitions (DB): 2.0.3.384 (green checkmark)
 - Asset management: 2.0.0.3 (green checkmark)
 - ITScripts: 4.0.76.4 (green checkmark)

- Phần 4: Rà quét và khắc phục lỗ hổng

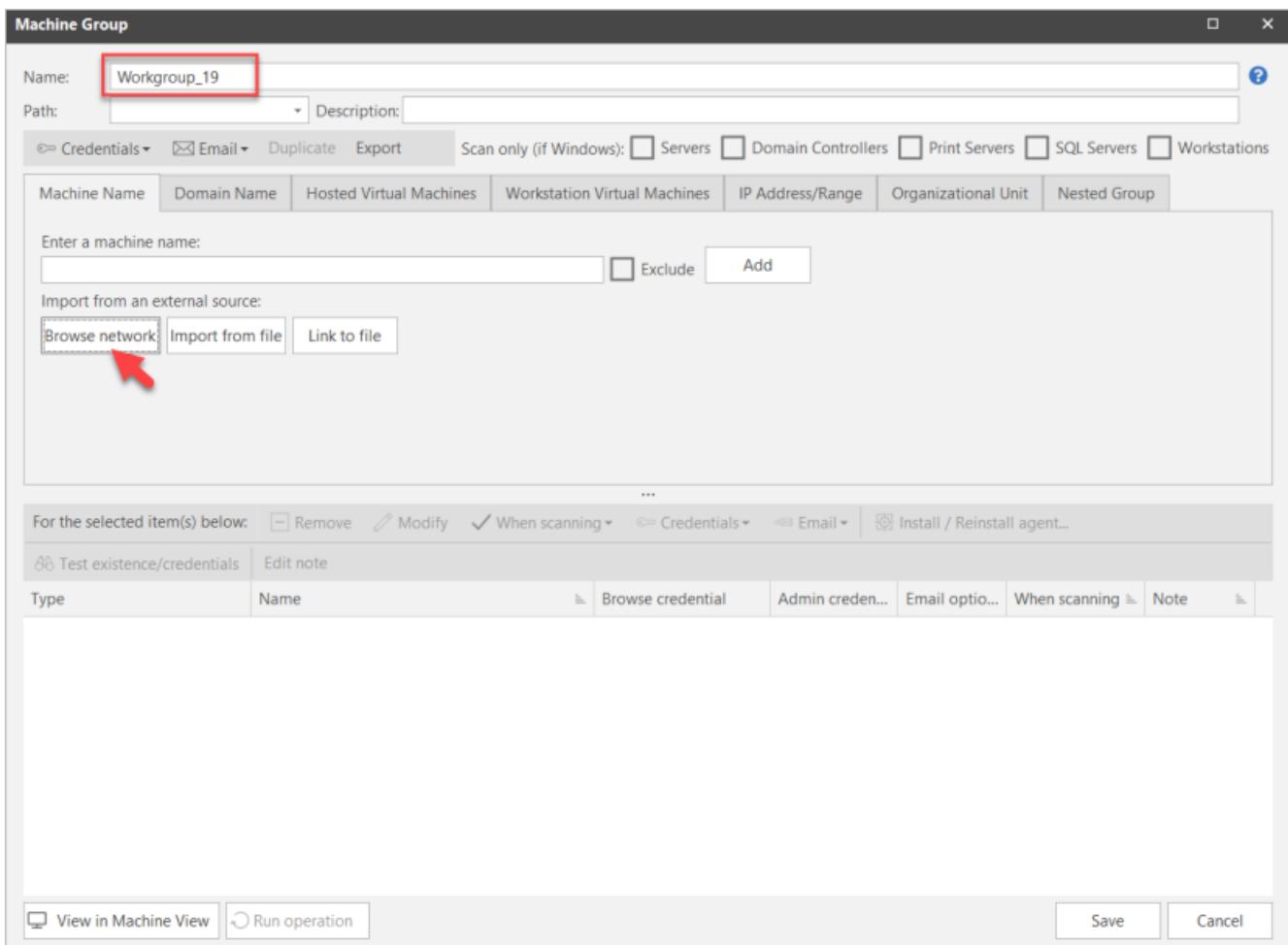
Dưới đây là các bước để thiết lập và thực hiện rà quét:

Tạo nhóm máy (Machine Group):

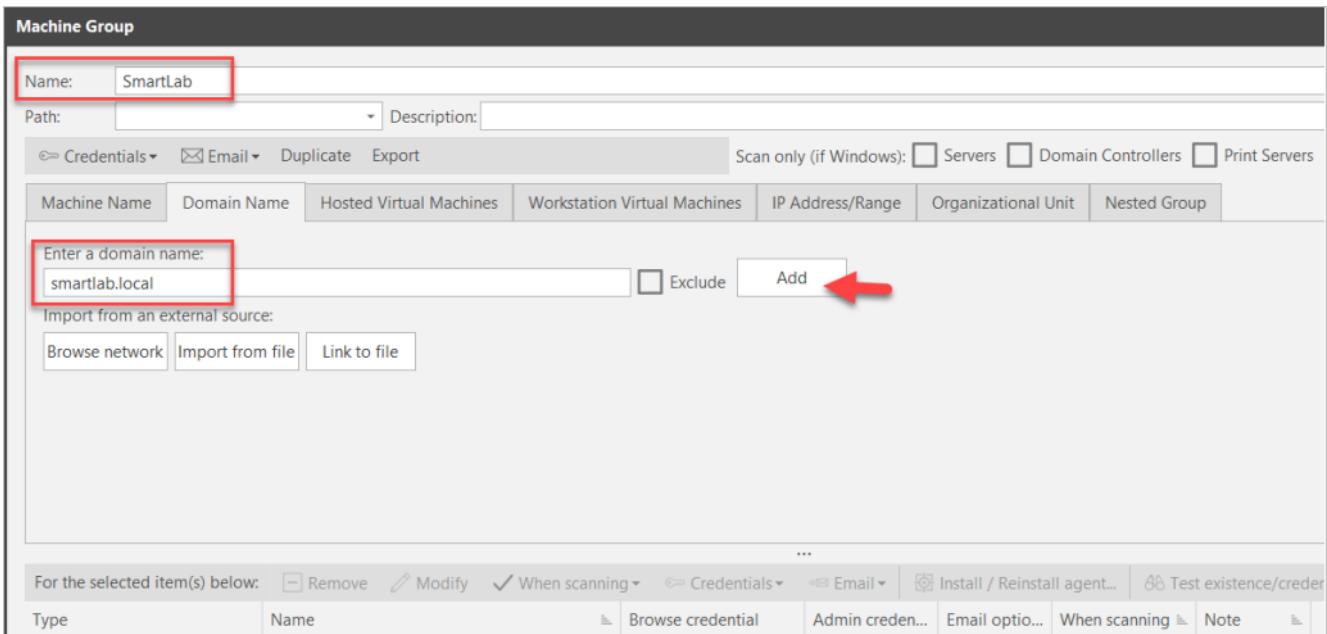
- Mở Machine Groups > Chọn New Machine Group.



- Đặt tên nhóm (ví dụ: SmartLab).
- Chọn **Browse network** để thêm máy vào nhóm.



- Nhập tên domain (nếu có, ví dụ: smartlab.local).



Machine Group

Name: SmartLab

Path: Description:

Credentials Email Duplicate Export Scan only (if Windows): Servers Domain Controllers Print Servers

Machine Name	Domain Name	Hosted Virtual Machines	Workstation Virtual Machines	IP Address/Range	Organizational Unit	Nested Group
	Enter a domain name: smartlab.local					

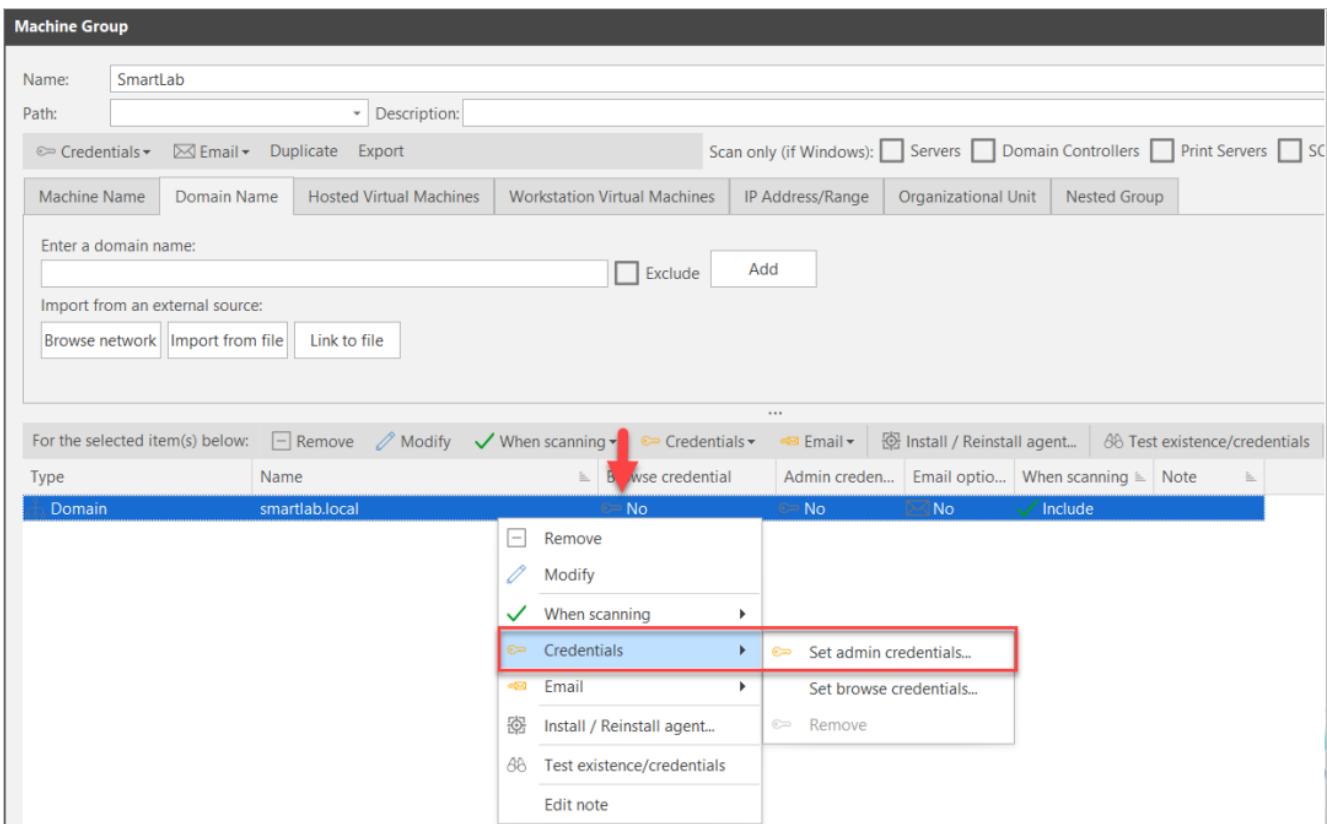
Import from an external source:
 Browse network Import from file Link to file

For the selected item(s) below: Remove Modify When scanning Credentials Email Install / Reinstall agent... Test existence/credentials

Type	Name	Browse credential	Admin creden...	Email optio...	When scanning	Note
Domain	smartlab.local	No	No	No	Include	

Thiết lập thông tin xác thực (Credentials):

- Trong Machine Group, chọn Credentials > Set admin credentials.



Machine Group

Name: SmartLab

Path: Description:

Credentials Email Duplicate Export Scan only (if Windows): Servers Domain Controllers Print Servers

Machine Name	Domain Name	Hosted Virtual Machines	Workstation Virtual Machines	IP Address/Range	Organizational Unit	Nested Group
	Enter a domain name: smartlab.local					

Import from an external source:
 Browse network Import from file Link to file

For the selected item(s) below: Remove Modify When scanning Credentials Email Install / Reinstall agent... Test existence/credentials

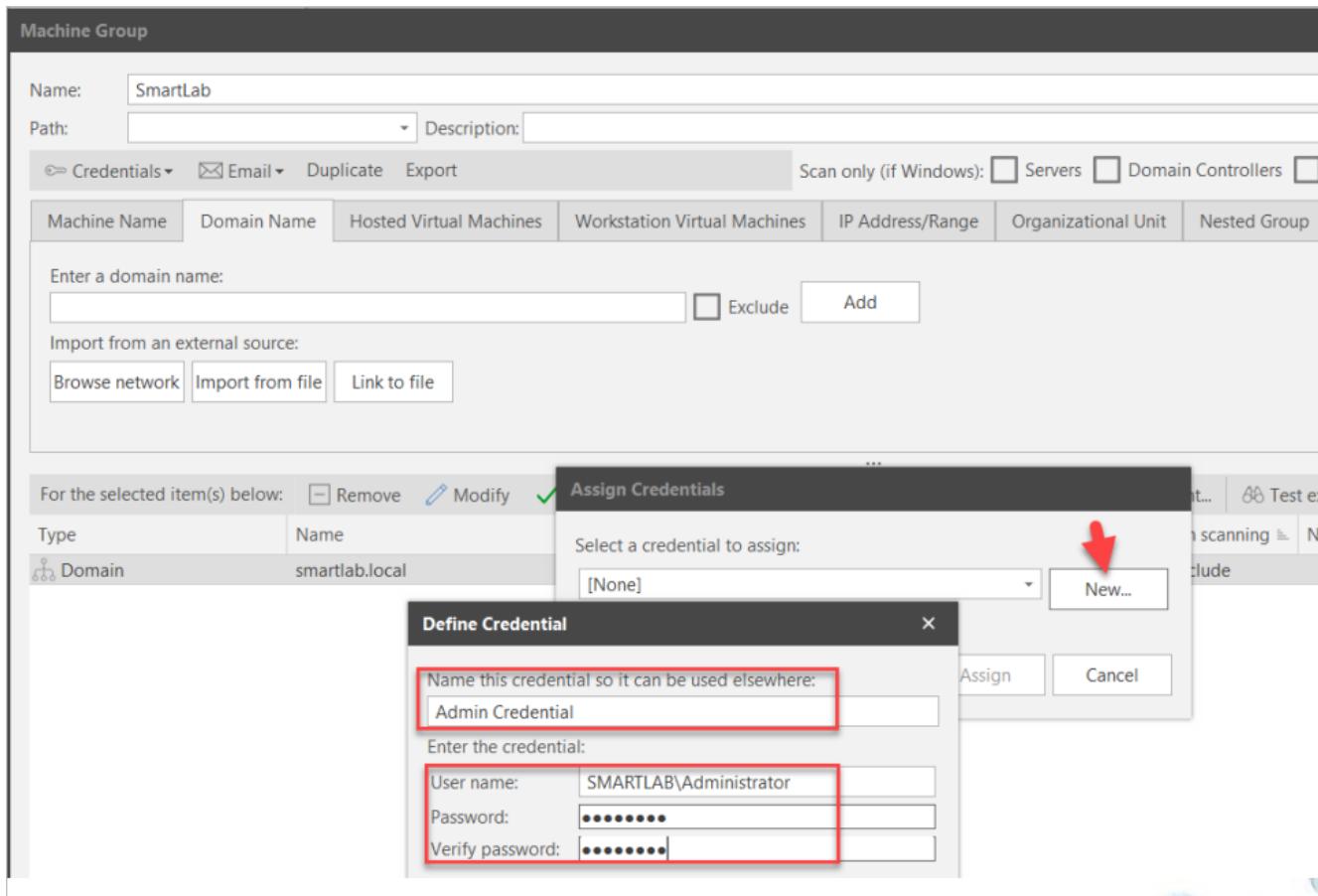
Type	Name	Browse credential	Admin creden...	Email optio...	When scanning	Note
Domain	smartlab.local	No	No	No	Include	

smartlab.local

Remove
Modify
When scanning
Credentials
Email
Install / Reinstall agent...
Test existence/credentials
Edit note

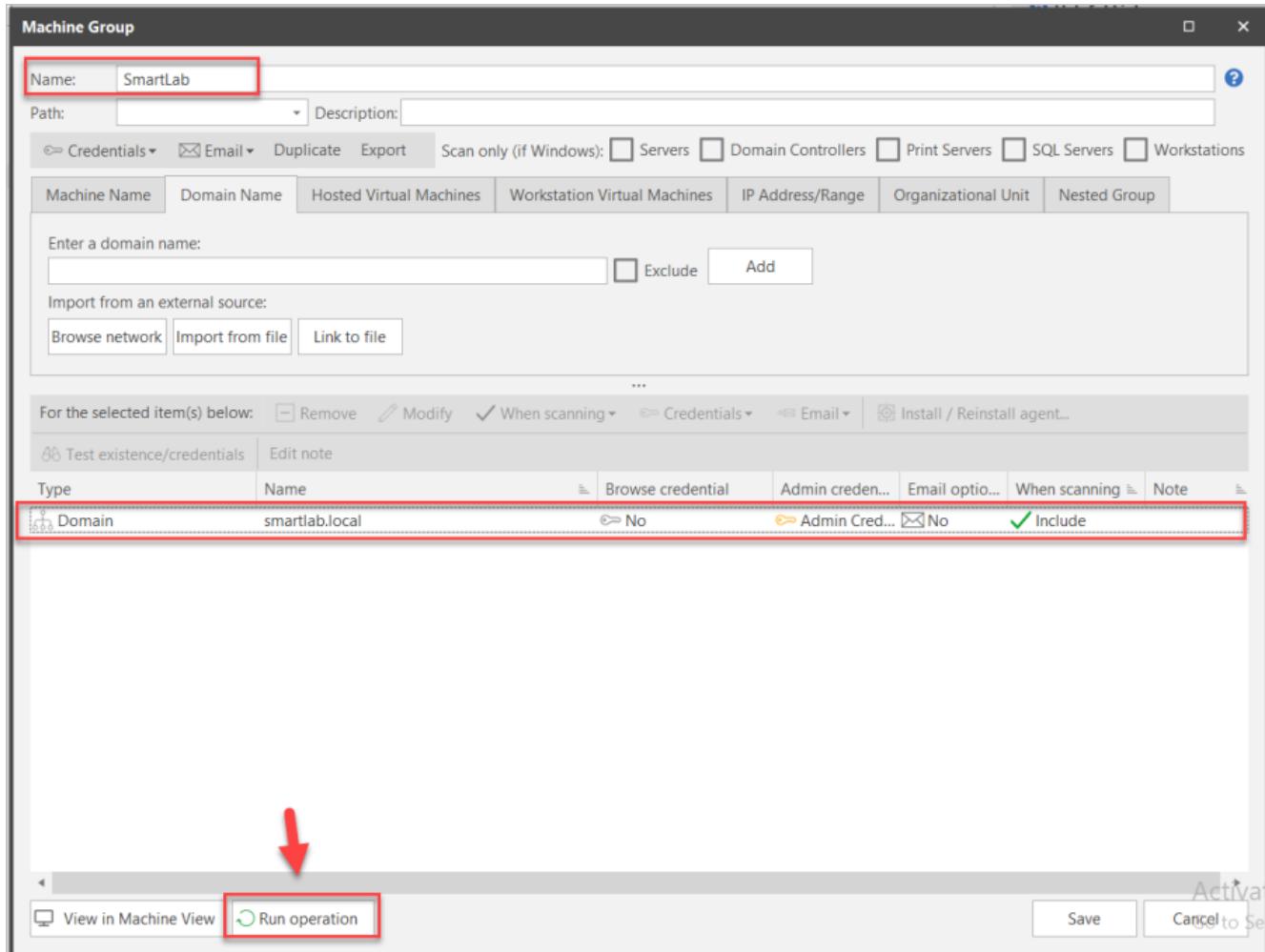
Set admin credentials...
Set browse credentials...
Remove

- Chọn **New**, nhập:
 - **User name:** Tên quản trị viên.
 - **Password:** Mật khẩu tương ứng.
 - Nhấn **OK**.

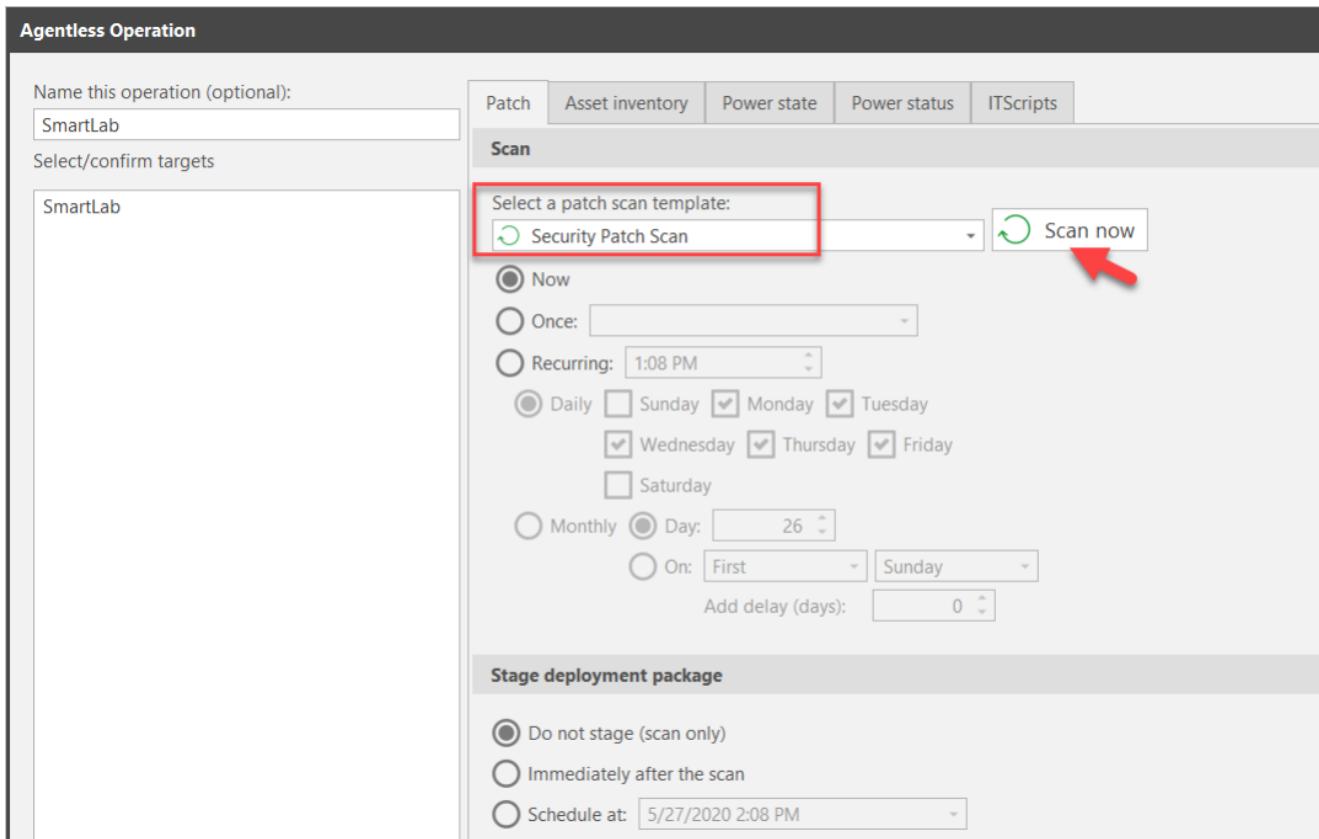


Chạy rà quét:

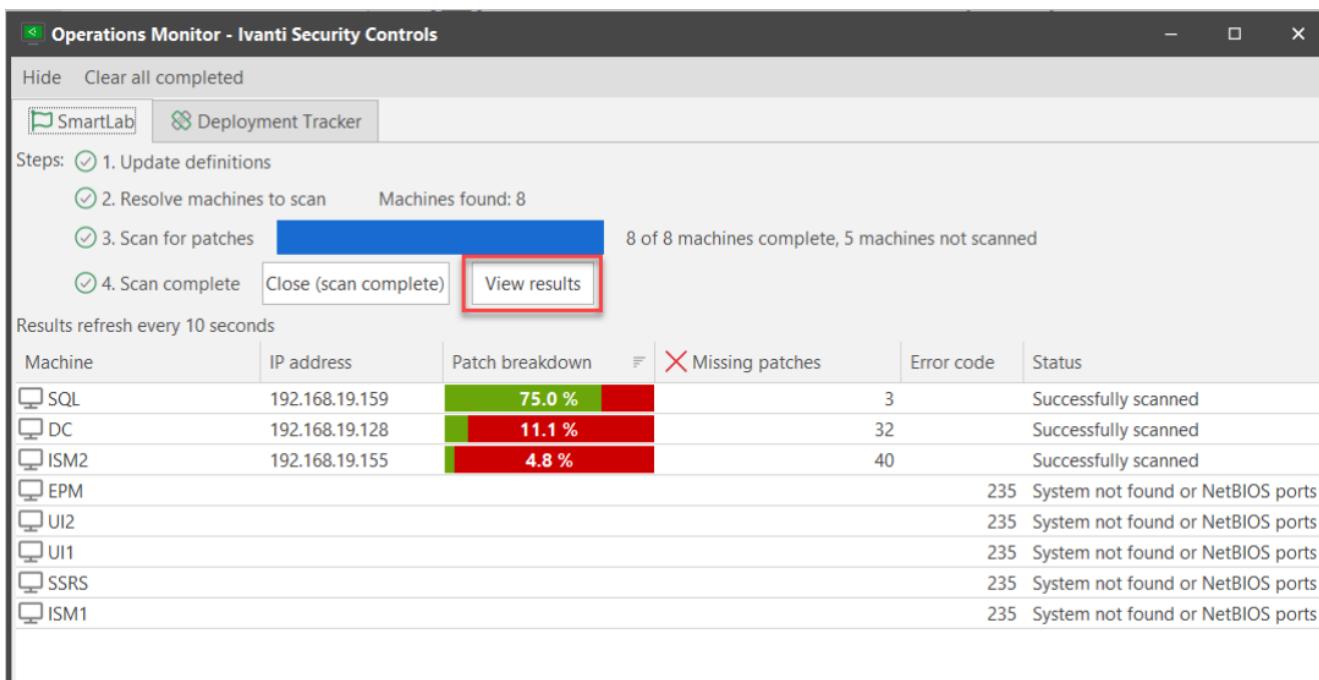
- Trong Machine Group, nhấp Run operation.



- Chọn Security Patch Scan > Scan now.



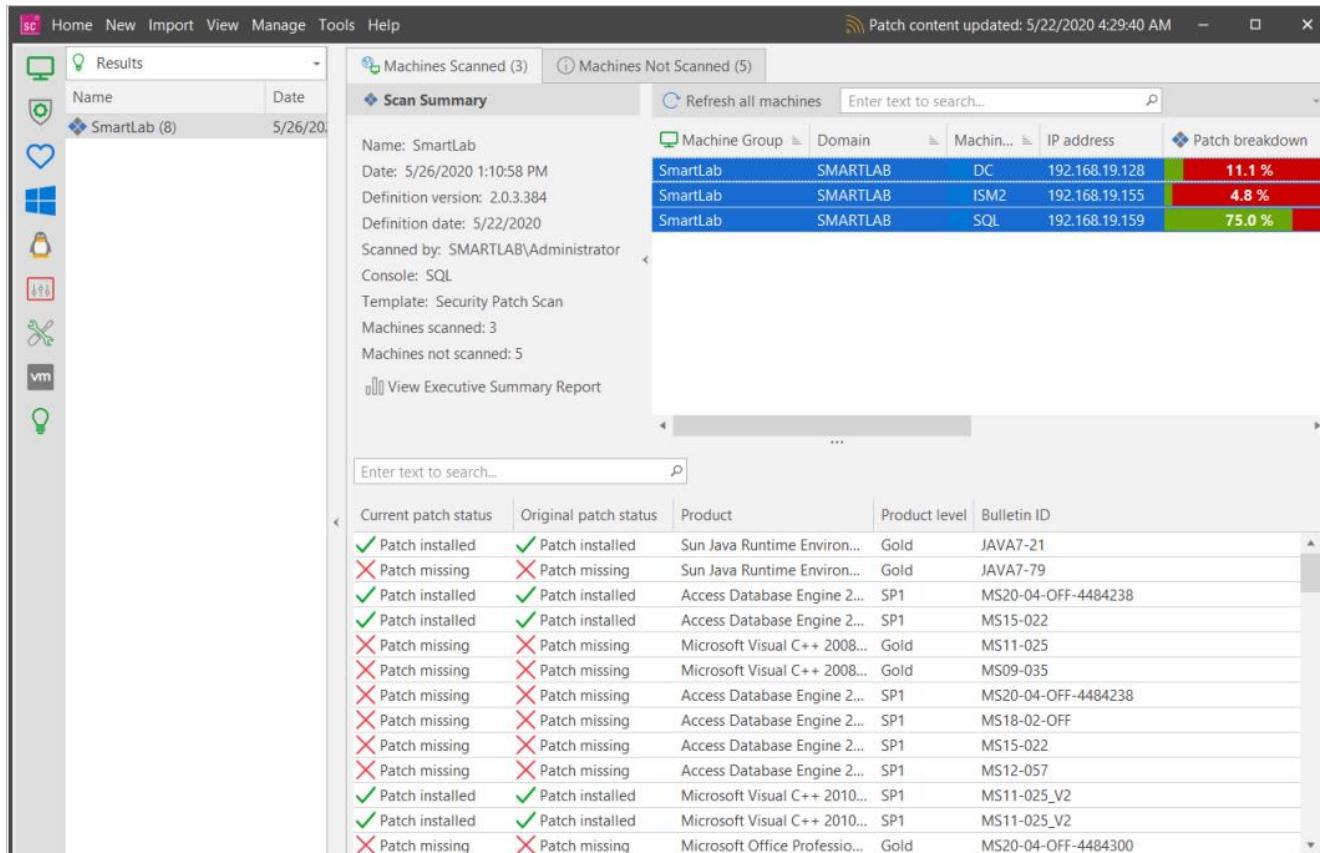
- Chờ quá trình quét hoàn tất, sau đó chọn View results.



Machine	IP address	Patch breakdown	Missing patches	Error code	Status
SQL	192.168.19.159	75.0 %	3	235	Successfully scanned
DC	192.168.19.128	11.1 %	32	235	System not found or NetBIOS ports
ISM2	192.168.19.155	4.8 %	40	235	System not found or NetBIOS ports
EPM				235	System not found or NetBIOS ports
UI2				235	System not found or NetBIOS ports
UI1				235	System not found or NetBIOS ports
SSRS				235	System not found or NetBIOS ports
ISM1				235	System not found or NetBIOS ports

Xem kết quả quét:

- Kết quả hiển thị danh sách máy với thông tin IP, số bản vá bị thiếu, trạng thái quét.

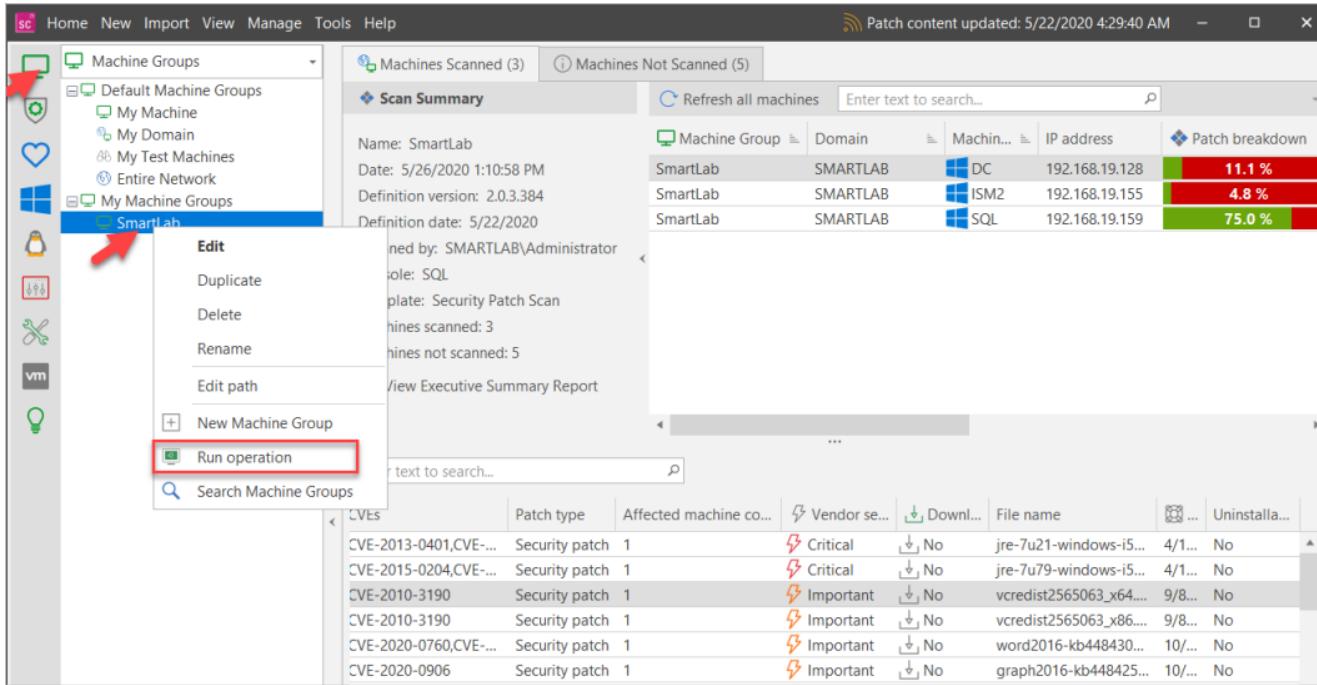


The screenshot shows the SmartPro software interface for managing assets and performing security scans. The main window displays a 'Scan Summary' for a machine named 'SmartLab'. The summary includes details such as the date (5/26/2020), definition version (2.0.3.384), and definition date (5/22/2020). It also shows the scanned by user (SMARTLAB\Administrator), console (SQL), and template (Security Patch Scan). The 'Machines Scanned' section shows three machines: SmartLab (Machine Group: SMARTLAB, Domain: DC, IP address: 192.168.19.128, Patch breakdown: 11.1%), SmartLab (Machine Group: SMARTLAB, Domain: ISM2, IP address: 192.168.19.155, Patch breakdown: 4.8%), and SmartLab (Machine Group: SMARTLAB, Domain: SQL, IP address: 192.168.19.159, Patch breakdown: 75.0%). Below the summary is a large table detailing the patch status for each machine across various products and bulletins. The table columns include Current patch status, Original patch status, Product, Product level, and Bulletin ID. The data shows a mix of 'Patch installed' (green checkmark) and 'Patch missing' (red X) status for different Microsoft products like Java Runtime Environment, Access Database Engine, and Microsoft Visual C++.

Current patch status	Original patch status	Product	Product level	Bulletin ID
✓ Patch installed	✓ Patch installed	Sun Java Runtime Environ...	Gold	JAVA7-21
✗ Patch missing	✗ Patch missing	Sun Java Runtime Environ...	Gold	JAVA7-79
✓ Patch installed	✓ Patch installed	Access Database Engine 2...	SP1	MS20-04-OFF-4484238
✓ Patch installed	✓ Patch installed	Access Database Engine 2...	SP1	MS15-022
✗ Patch missing	✗ Patch missing	Microsoft Visual C++ 2008...	Gold	MS11-025
✗ Patch missing	✗ Patch missing	Microsoft Visual C++ 2008...	Gold	MS09-035
✗ Patch missing	✗ Patch missing	Access Database Engine 2...	SP1	MS20-04-OFF-4484238
✗ Patch missing	✗ Patch missing	Access Database Engine 2...	SP1	MS18-02-OFF
✗ Patch missing	✗ Patch missing	Access Database Engine 2...	SP1	MS15-022
✗ Patch missing	✗ Patch missing	Access Database Engine 2...	SP1	MS12-057
✓ Patch installed	✓ Patch installed	Microsoft Visual C++ 2010...	SP1	MS11-025_V2
✓ Patch installed	✓ Patch installed	Microsoft Visual C++ 2010...	SP1	MS11-025_V2
✗ Patch missing	✗ Patch missing	Microsoft Office Professio...	Gold	MS20-04-OFF-4484300

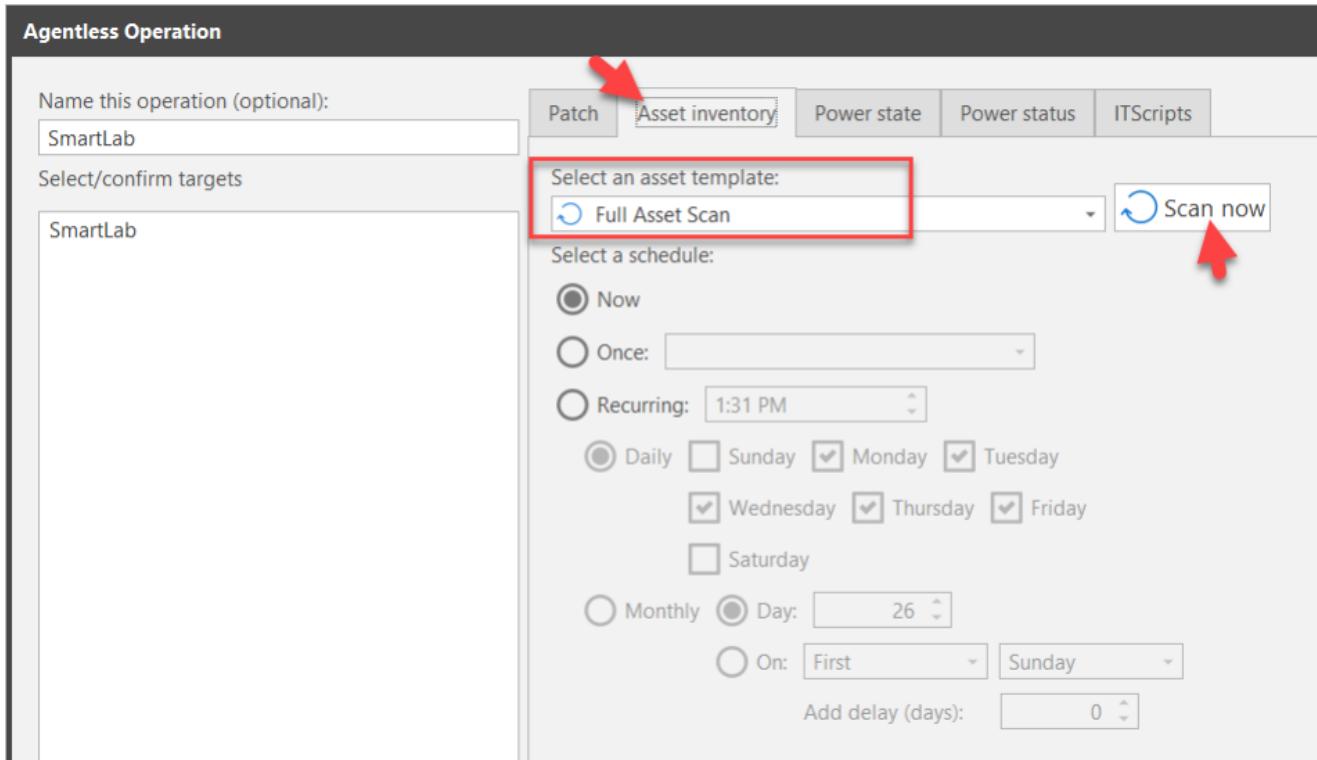
Quét tài sản (Asset Inventory):

- Mở lại Run operation.



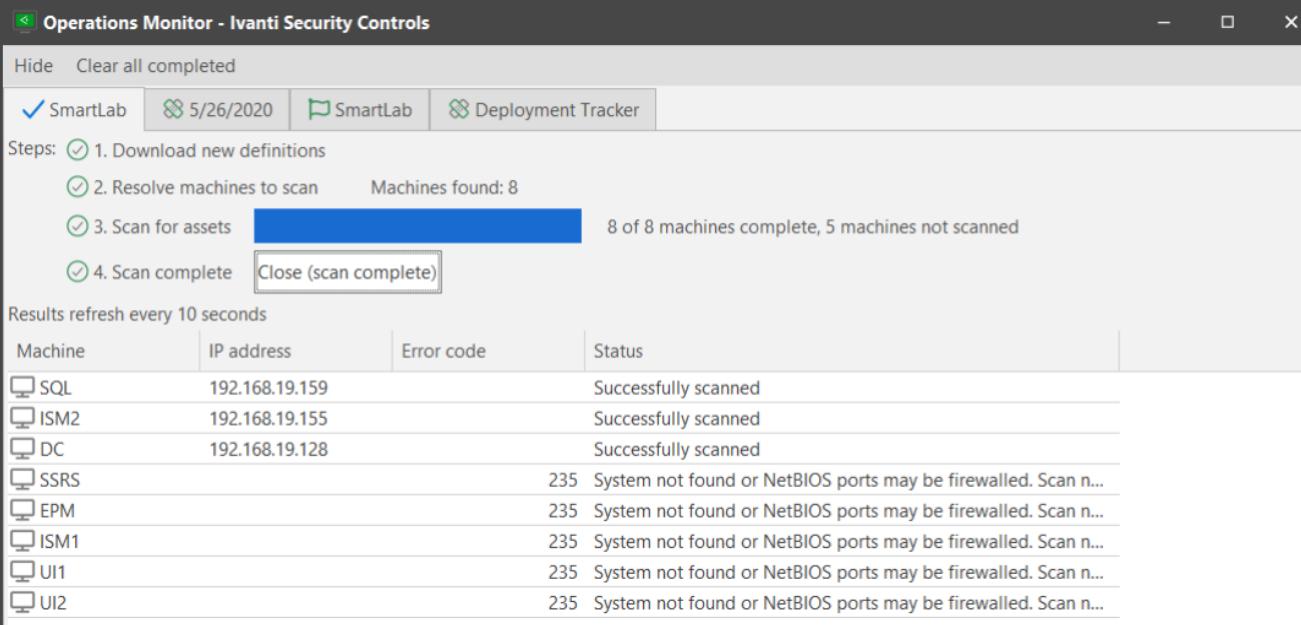
The screenshot shows the SmartPro Asset Management software interface. On the left, there's a sidebar with various icons and a tree view of machine groups. A red arrow points to the 'SmartLab' group in the 'My Machine Groups' section. A context menu is open over this group, with a red box highlighting the 'Run operation' option. The main pane displays a 'Scan Summary' for 'SmartLab', showing details like Name: SmartLab, Date: 5/26/2020 1:10:58 PM, and Definition version: 2.0.3.384. Below this is a table of scanned machines, and at the bottom is a list of vulnerabilities (CVEs) with their patch status.

- Chọn Asset Inventory > Full Asset Scan > Scan now.



The screenshot shows the 'Agentless Operation' dialog box. It has tabs for Patch, Asset inventory, Power state, Power status, and ITScripts. The 'Asset inventory' tab is active. A red box highlights the 'Select an asset template:' dropdown, which shows 'Full Asset Scan' selected. A red arrow points to the 'Scan now' button, which is located at the bottom right of the dialog. The dialog also includes fields for naming the operation (optional), selecting targets (a list box showing 'SmartLab'), scheduling the scan (with options for Now, Once, Recurring, Daily, Weekly, Monthly, or On specific dates), and adding a delay.

- Sau khi quét xong, xem kết quả trong Operations Monitor.



Operations Monitor - Ivanti Security Controls

Hide Clear all completed

SmartLab 5/26/2020 SmartLab Deployment Tracker

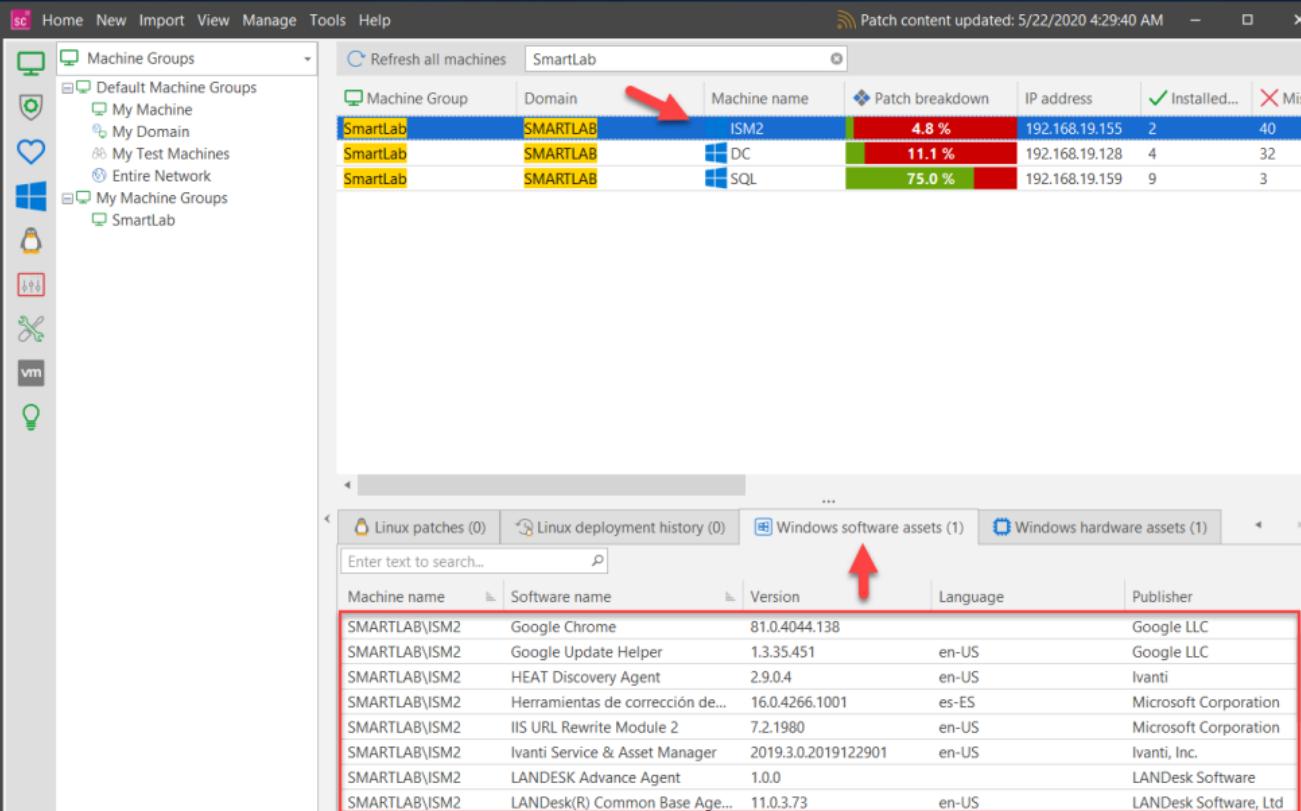
Steps: 1. Download new definitions
 2. Resolve machines to scan Machines found: 8
 3. Scan for assets 8 of 8 machines complete, 5 machines not scanned
 4. Scan complete Close (scan complete)

Results refresh every 10 seconds

Machine	IP address	Error code	Status
SQL	192.168.19.159		Successfully scanned
ISM2	192.168.19.155		Successfully scanned
DC	192.168.19.128		Successfully scanned
SSRS		235	System not found or NetBIOS ports may be firewalled. Scan n...
EPM		235	System not found or NetBIOS ports may be firewalled. Scan n...
ISM1		235	System not found or NetBIOS ports may be firewalled. Scan n...
UI1		235	System not found or NetBIOS ports may be firewalled. Scan n...
UI2		235	System not found or NetBIOS ports may be firewalled. Scan n...

Phân tích chi tiết:

- Trong kết quả quét, chọn từng máy:
 - Tab Windows software assets: Xem phần mềm cài đặt.



sc Home New Import View Manage Tools Help Patch content updated: 5/22/2020 4:29:40 AM

Machine Groups

- Default Machine Groups
 - My Machine
 - My Domain
 - My Test Machines
 - Entire Network
- My Machine Groups
 - SmartLab

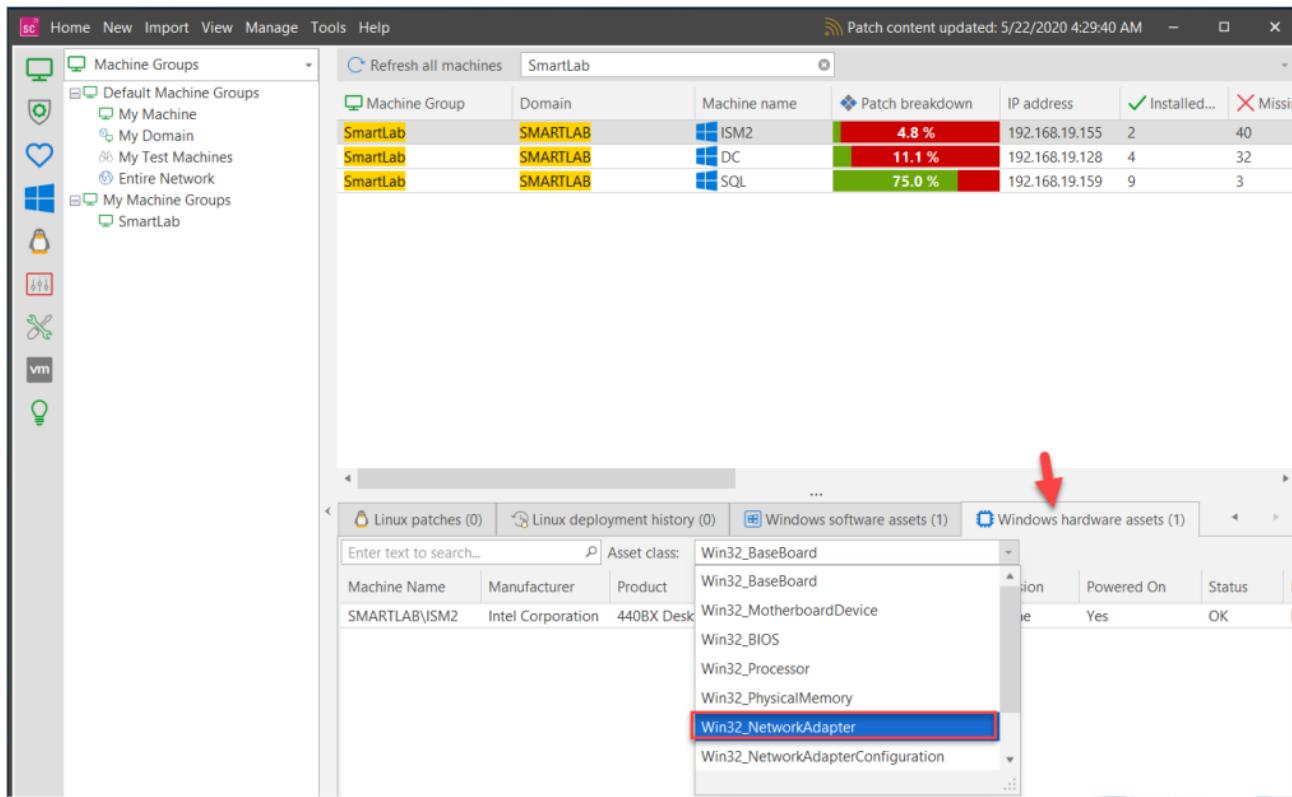
Refresh all machines SmartLab

Machine Group	Domain	Machine name	Patch breakdown	IP address	Installed...	Missing
SmartLab	SMARTLAB	ISM2	4.8 %	192.168.19.155	2	40
SmartLab	SMARTLAB	DC	11.1 %	192.168.19.128	4	32
SmartLab	SMARTLAB	SQL	75.0 %	192.168.19.159	9	3

Linux patches (0) Linux deployment history (0) Windows software assets (1) Windows hardware assets (1)

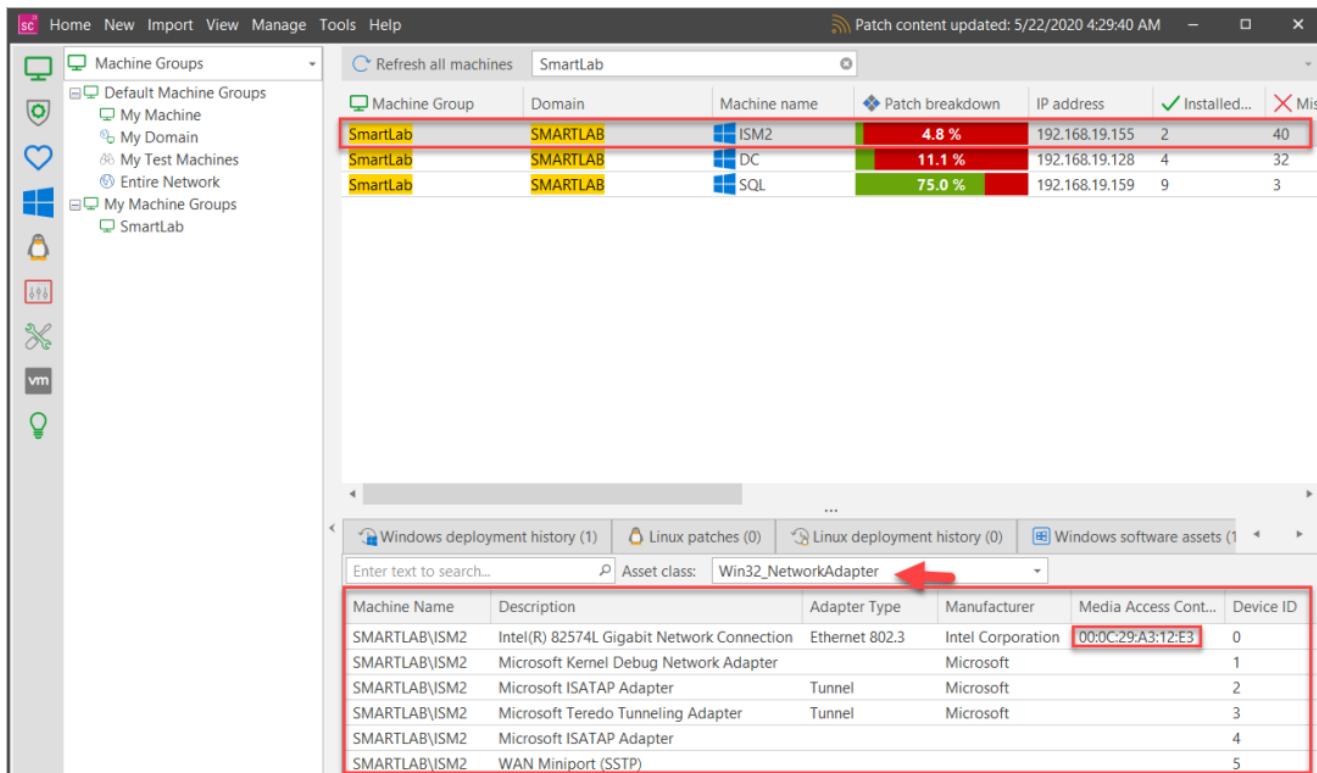
Machine name	Software name	Version	Language	Publisher
SMARTLAB\ISM2	Google Chrome	81.0.4044.138		Google LLC
SMARTLAB\ISM2	Google Update Helper	1.33.451	en-US	Google LLC
SMARTLAB\ISM2	HEAT Discovery Agent	2.9.0.4	en-US	Ivanti
SMARTLAB\ISM2	Herramientas de corrección de...	16.0.4266.1001	es-ES	Microsoft Corporation
SMARTLAB\ISM2	IIS URL Rewrite Module 2	7.2.1980	en-US	Microsoft Corporation
SMARTLAB\ISM2	Ivanti Service & Asset Manager	2019.3.0.2019122901	en-US	Ivanti, Inc.
SMARTLAB\ISM2	LANDesk Advance Agent	1.0.0		LANDesk Software
SMARTLAB\ISM2	LANDesk(R) Common Base Age...	11.0.3.73	en-US	LANDesk Software, Ltd

➤ Tab Windows hardware assets: Xem tài nguyên phần cứng.



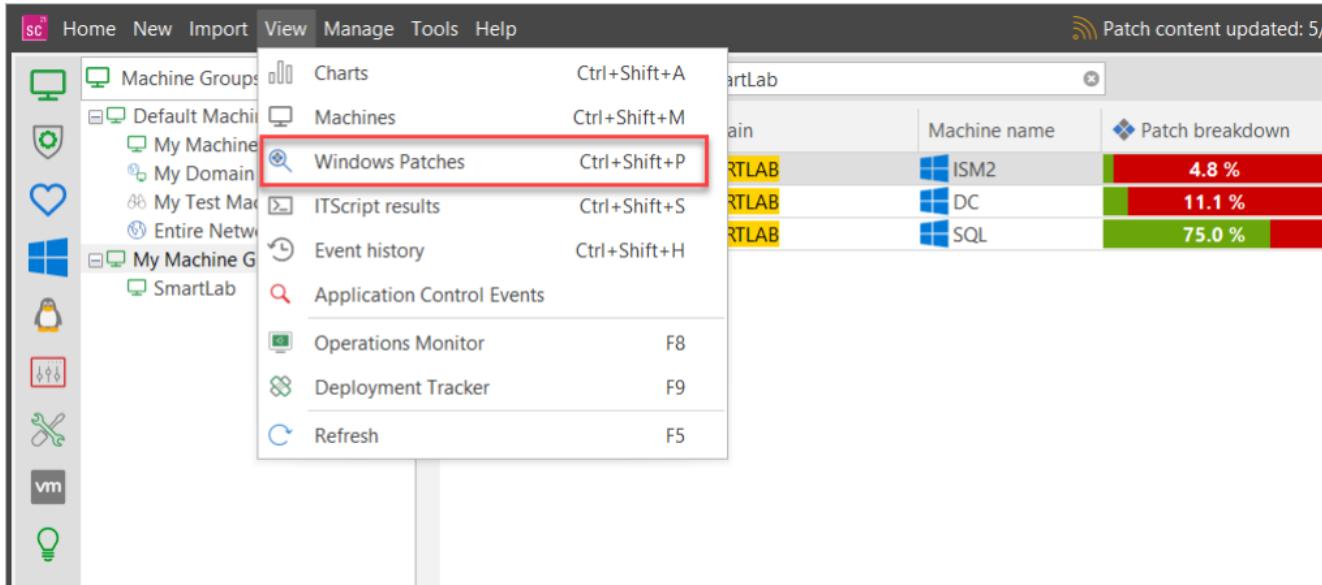
Asset class:	Win32_BaseBoard
Machine Name	SMARTLAB\ISM2
Manufacturer	Intel Corporation
Product	440BX Desk
	Win32_MotherboardDevice
	Win32_BIOS
	Win32_Processor
	Win32_PhysicalMemory
	Win32_NetworkAdapter
	Win32_NetworkAdapterConfiguration

- Xem thông tin tài nguyên của máy cụ thể (ví dụ: ISM2).



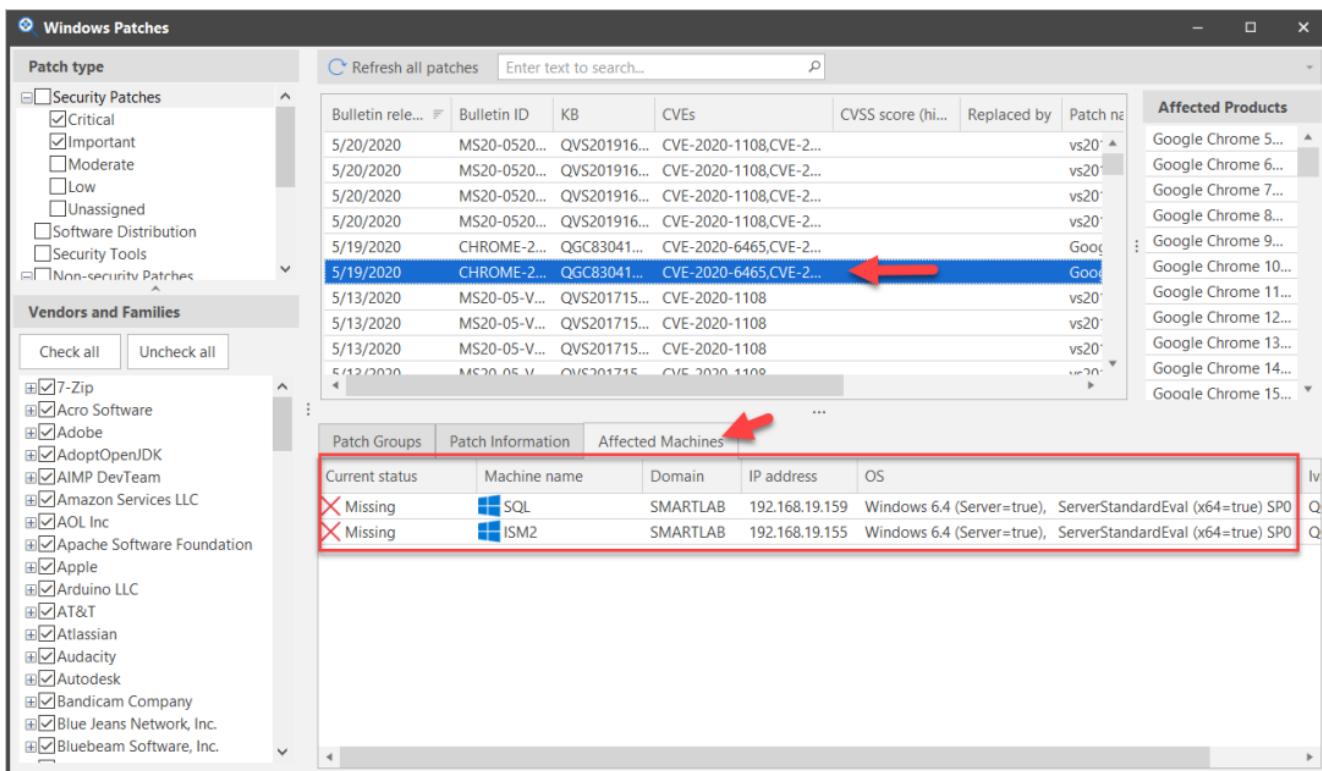
Machine Name	Description	Adapter Type	Manufacturer	Media Access Cont...	Device ID
SMARTLAB\ISM2	Intel(R) 82574L Gigabit Network Connection	Ethernet 802.3	Intel Corporation	00:0C:29:A3:12:E3	0
SMARTLAB\ISM2	Microsoft Kernel Debug Network Adapter		Microsoft		1
SMARTLAB\ISM2	Microsoft ISATAP Adapter	Tunnel	Microsoft		2
SMARTLAB\ISM2	Microsoft Teredo Tunneling Adapter	Tunnel	Microsoft		3
SMARTLAB\ISM2	Microsoft ISATAP Adapter				4
SMARTLAB\ISM2	WAN Miniport (SSTP)				5

- Xem danh sách bản vá và lỗi của Windows.



Chọn bản vá:

- Trong tab **Patch**, chọn các bản vá cần áp dụng từ danh sách (ví dụ: Security Patches từ các nhà cung cấp như Microsoft, Adobe...).

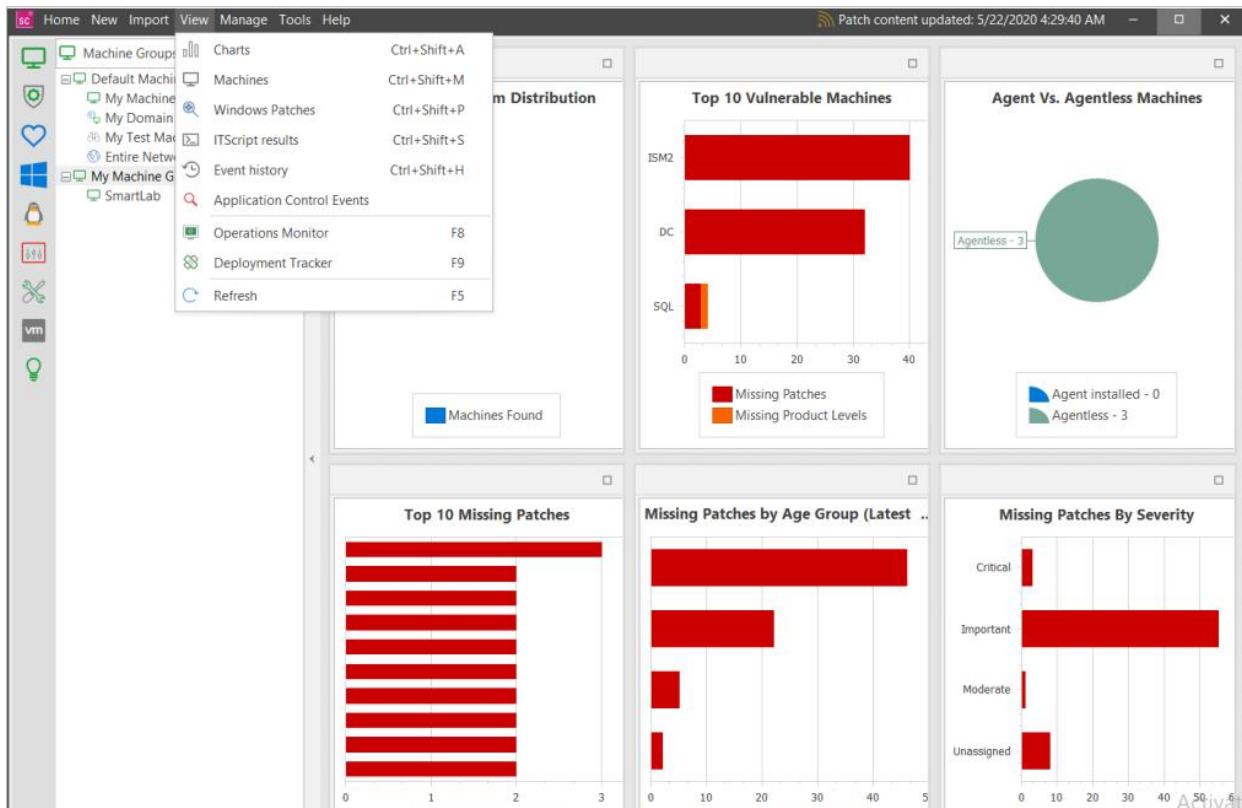


The screenshot shows the 'Windows Patches' window with the following details:

- Patch type:** Security Patches (selected), Critical, Important, Moderate, Low, Unassigned, Software Distribution, Security Tools, Non-security Patches.
- Vendors and Families:** 7-Zip, Acro Software, Adobe, AdoptOpenJDK, AIMP DevTeam, Amazon Services LLC, AOL Inc, Apache Software Foundation, Apple, Arduino LLC, AT&T, Atlassian, Audacity, Autodesk, Bandicam Company, Blue Jeans Network, Inc., Bluebeam Software, Inc.
- Affected Products:** Google Chrome 5..., Google Chrome 6..., Google Chrome 7..., Google Chrome 8..., Google Chrome 9..., Google Chrome 10..., Google Chrome 11..., Google Chrome 12..., Google Chrome 13..., Google Chrome 14..., Google Chrome 15...
- Patch Groups:** Patch Information, Affected Machines (highlighted with a red box).
- Affected Machines:** Current status: Missing (for SQL and ISM2), Machine name: SQL, ISM2, Domain: SMARTLAB, IP address: 192.168.19.159, OS: Windows 6.4 (Server=true), ServerStandardEval (x64=true) SP0.

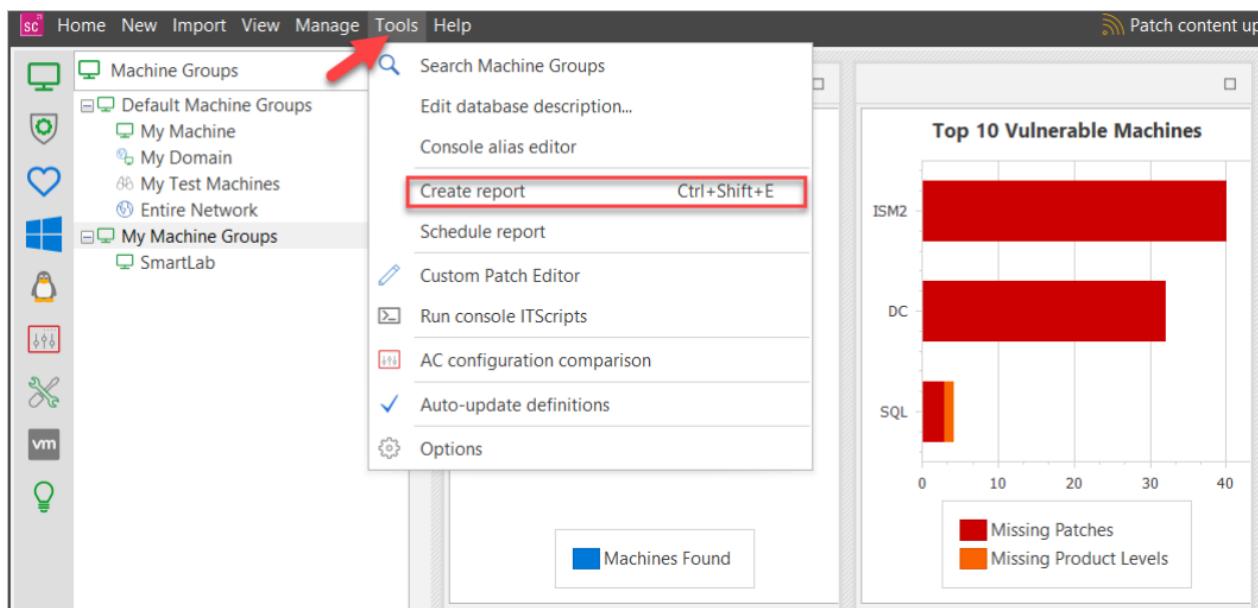
Xem biểu đồ:

- Chọn View > Charts để xem biểu đồ phân tích lỗ hổng.

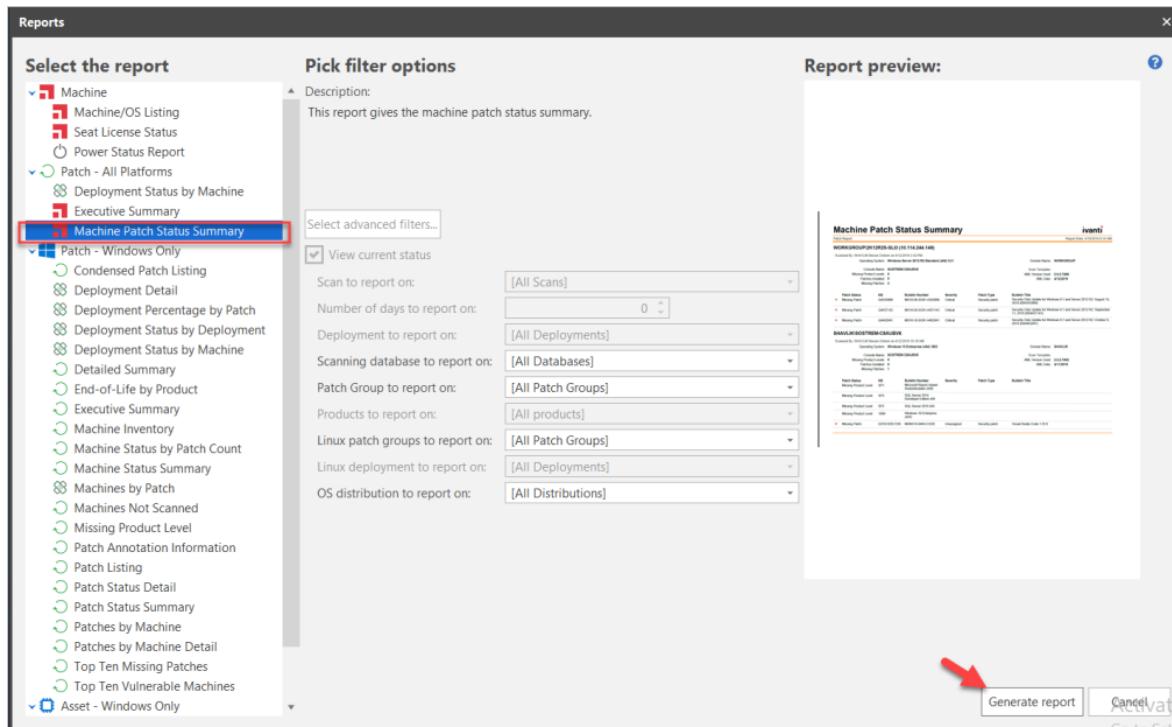


Tạo báo cáo:

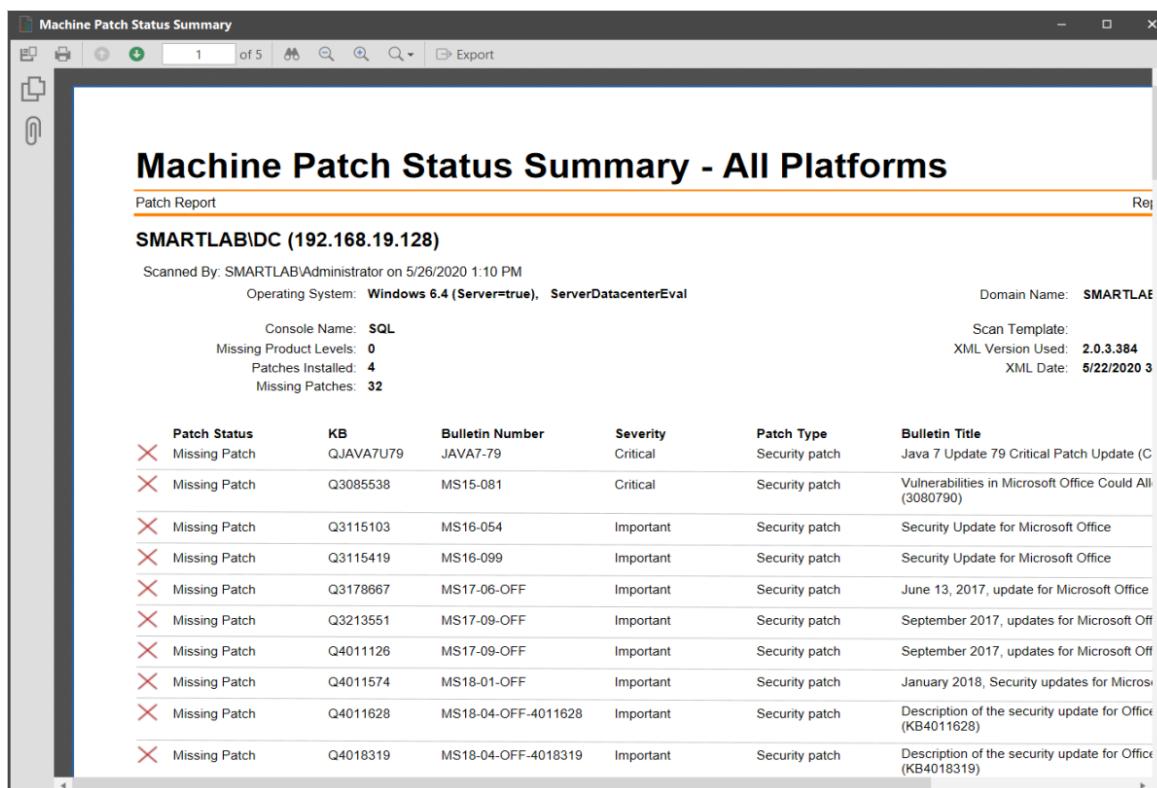
- Chọn Tools > Create report.



- Chọn Machine Patch Status Summary > Generate report.



- Báo cáo hiển thị chi tiết trạng thái bản vá của từng máy (ví dụ: SMARTLAB\DC với 32 bản vá bị thiếu).



Machine Patch Status Summary - All Platforms

Patch Report

SMARTLAB\DC (192.168.19.128)

Scanned By: SMARTLAB\Administrator on 5/26/2020 1:10 PM

Operating System: Windows 6.4 (Server=true), ServerDatacenterEval

Domain Name: SMARTLAB

Console Name: SQL

Missing Product Levels: 0

Patches Installed: 4

Missing Patches: 32

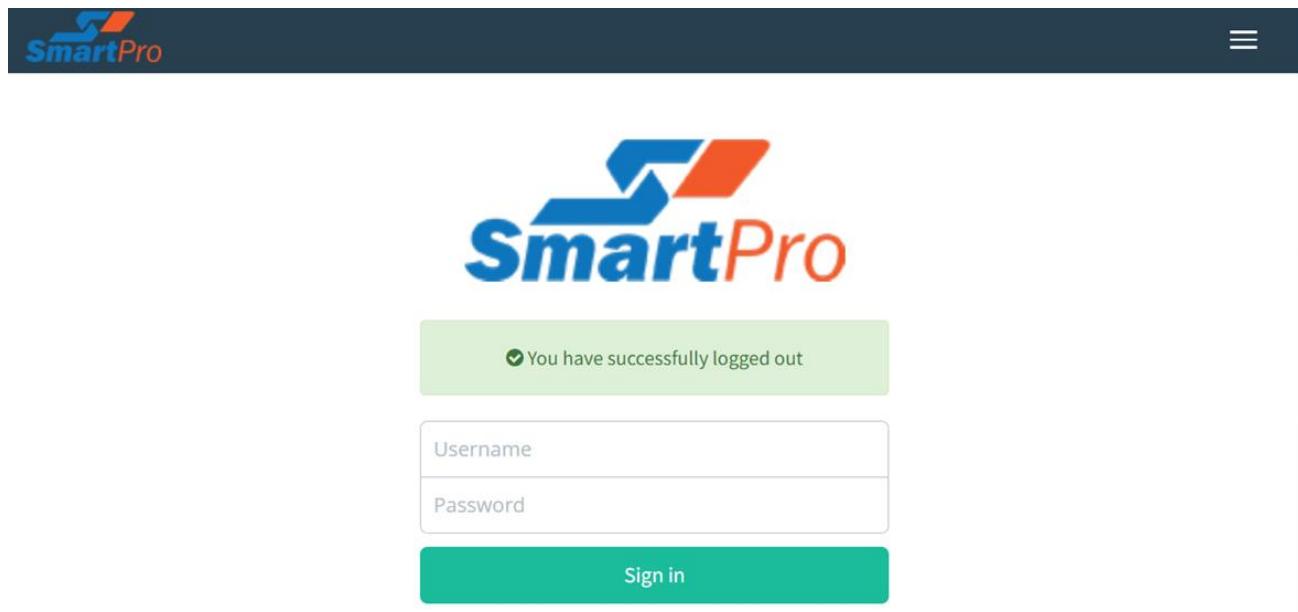
Patch Status	KB	Bulletin Number	Severity	Patch Type	Bulletin Title
Missing Patch	QJAVA7U79	JAVA7-79	Critical	Security patch	Java 7 Update 79 Critical Patch Update (C
Missing Patch	Q3085538	MS15-081	Critical	Security patch	Vulnerabilities in Microsoft Office Could All (3080790)
Missing Patch	Q3115103	MS16-054	Important	Security patch	Security Update for Microsoft Office
Missing Patch	Q3115419	MS16-099	Important	Security patch	Security Update for Microsoft Office
Missing Patch	Q3178667	MS17-06-OFF	Important	Security patch	June 13, 2017, update for Microsoft Office
Missing Patch	Q3213551	MS17-09-OFF	Important	Security patch	September 2017, updates for Microsoft Off
Missing Patch	Q4011126	MS17-09-OFF	Important	Security patch	September 2017, updates for Microsoft Off
Missing Patch	Q4011574	MS18-01-OFF	Important	Security patch	January 2018, Security updates for Micros
Missing Patch	Q4011628	MS18-04-OFF-4011628	Important	Security patch	Description of the security update for Office (KB4011628)
Missing Patch	Q4018319	MS18-04-OFF-4018319	Important	Security patch	Description of the security update for Office (KB4018319)

5. Hướng dẫn sử dụng GoPhish

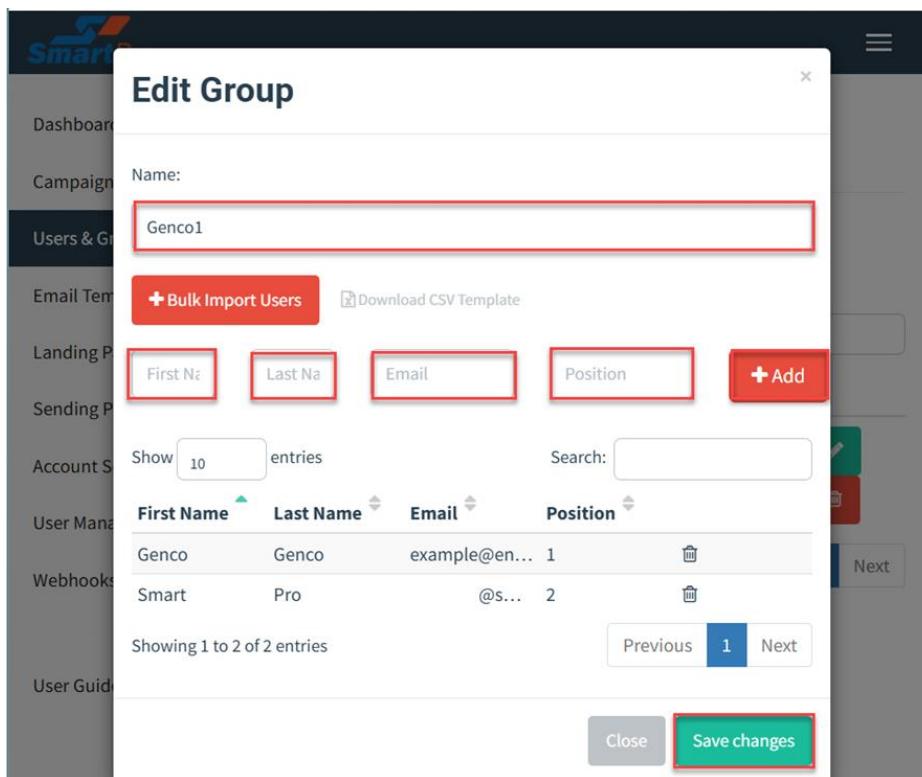
- Bước 1: Truy cập tool phishing của SmartPro theo đường dẫn sau:

<https://phishing.tek1.vn/>

Sử dụng tài khoản được cung cấp để đăng nhập



- Bước 2: Tạo User/Group. Đây sẽ là target tấn công của ta



The screenshot shows the "Edit Group" dialog box from the SmartPro application. The dialog has a title bar "Edit Group" and a close button. On the left is a sidebar with navigation links: Dashboard, Campaigns, Users & Groups (which is selected and highlighted in blue), Email Templates, Landing Pages, Sending Plans, Account Settings, User Management, Webhooks, and User Guide. The main content area contains the following elements:

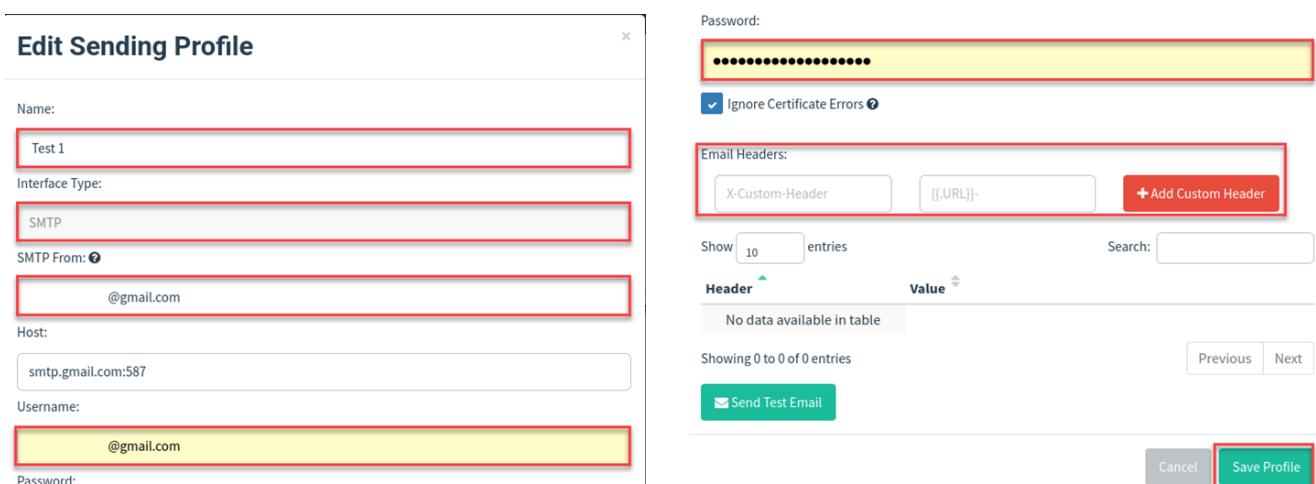
- A "Name:" label followed by an input field containing "Genco1".
- A red "Bulk Import Users" button and a "Download CSV Template" link.
- Four input fields labeled "First Name", "Last Name", "Email", and "Position", all of which are currently empty and highlighted with red boxes.
- A red "+ Add" button.
- A pagination section showing "Show 10 entries" and a "Search" input field.
- A table with two rows of data:

First Name	Last Name	Email	Position
Genco	Genco	example@example.com	1
Smart	Pro	@sample.com	2
- Pagination controls "Previous", "1", and "Next".
- Buttons at the bottom: "Close" and "Save changes" (which is highlighted with a red box).

- Bước 3: Tạo Send Profiles.

- Name: Tên hồ sơ gửi email.
- Interface Type: Giao thức gửi email (SMTP).
- SMTP From: Địa chỉ email hiển thị khi gửi.
- Host: Máy chủ SMTP (vd: smtp.gmail.com:587).
- Username & Password: Thông tin đăng nhập email.
- Ignore Certificate Errors: Bỏ qua lỗi chứng chỉ (nếu cần).
- Email Headers: Thêm tiêu đề tùy chỉnh vào email.

➤ Nhập thông tin và nhấn nút save profile



Edit Sending Profile

Name: Test 1

Interface Type: SMTP

SMTP From: @gmail.com

Host: smtp.gmail.com:587

Username: @gmail.com

Password: (Redacted)

Email Headers:

Header	Value
X-Custom-Header	([.URL]-)

Show 10 entries Search: Previous Next

No data available in table

Showing 0 to 0 of 0 entries

Send Test Email

Cancel Save Profile

Lưu ý: Không cung cấp mật khẩu Gmail, chỉ cung cấp app password.

- Bật Xác minh 2 bước tại Google Security.
- Vào App Passwords, đăng nhập lại nếu cần.
- Chọn Mail và thiết bị, hoặc chọn Other để nhập tên tùy chỉnh.
- Nhấn Generate, sao chép mật khẩu 16 ký tự và dùng thay cho mật khẩu Gmail khi cấu hình SMTP

Google Tài khoản

← Mật khẩu ứng dụng

Mật khẩu ứng dụng giúp bạn đăng nhập vào Tài khoản Google của mình trên những ứng dụng và dịch vụ cũ không hỗ trợ các tiêu chuẩn bảo mật hiện đại.

Mật khẩu ứng dụng kém an toàn hơn so với việc sử dụng những ứng dụng và dịch vụ mới nhất hỗ trợ các tiêu chuẩn bảo mật hiện đại. Trước khi tạo mật khẩu ứng dụng, bạn nên kiểm tra xem ứng dụng của mình có cần mật khẩu này để đăng nhập hay không.

[Tim hiểu thêm](#)

Mật khẩu ứng dụng của bạn

SMTP Mail (2)

Ngày tạo: 19 thg 2, Lần sử dụng gần đây nhất: 12 thg 3



SMTP Mail

Ngày tạo: 23 thg 12, 2024, Lần sử dụng gần đây nhất: 2 thg 1



Để tạo mật khẩu mới dành riêng cho ứng dụng, hãy nhập tên của ứng dụng đó vào bên dưới...

Tên ứng dụng

- Bước 4: Tạo Compaigns.

- **Name** – Tên chiến dịch.
- **Email Template** – Mẫu email gửi đến nạn nhân (tạo trong mục Email Templates).
- **Landing Page** – Trang đích khi nạn nhân nhấp vào liên kết (tạo trong Landing Pages).
- **URL** – Địa chỉ trang đích thay thế cho biến `{{.URL}}` trong email.
- **Launch Date** – Ngày bắt đầu chiến dịch.
- **Send Emails By** – Hạn chót gửi toàn bộ email.
- **Profile** – Cấu hình SMTP để gửi email (Sending Profiles).
- **Groups** – Nhóm người nhận mục tiêu của chiến dịch.

New Campaign

X

Name:

Genco1

Email Template:

Genco1

Landing Page:

Genco 1

URL: 

<https://genco1.smartpro.edu.vn>

Launch Date

March 11th 2025, 4:50 pm

Send Emails By (Optional) 

Sending Profile:

Test 1



 Send Test Email

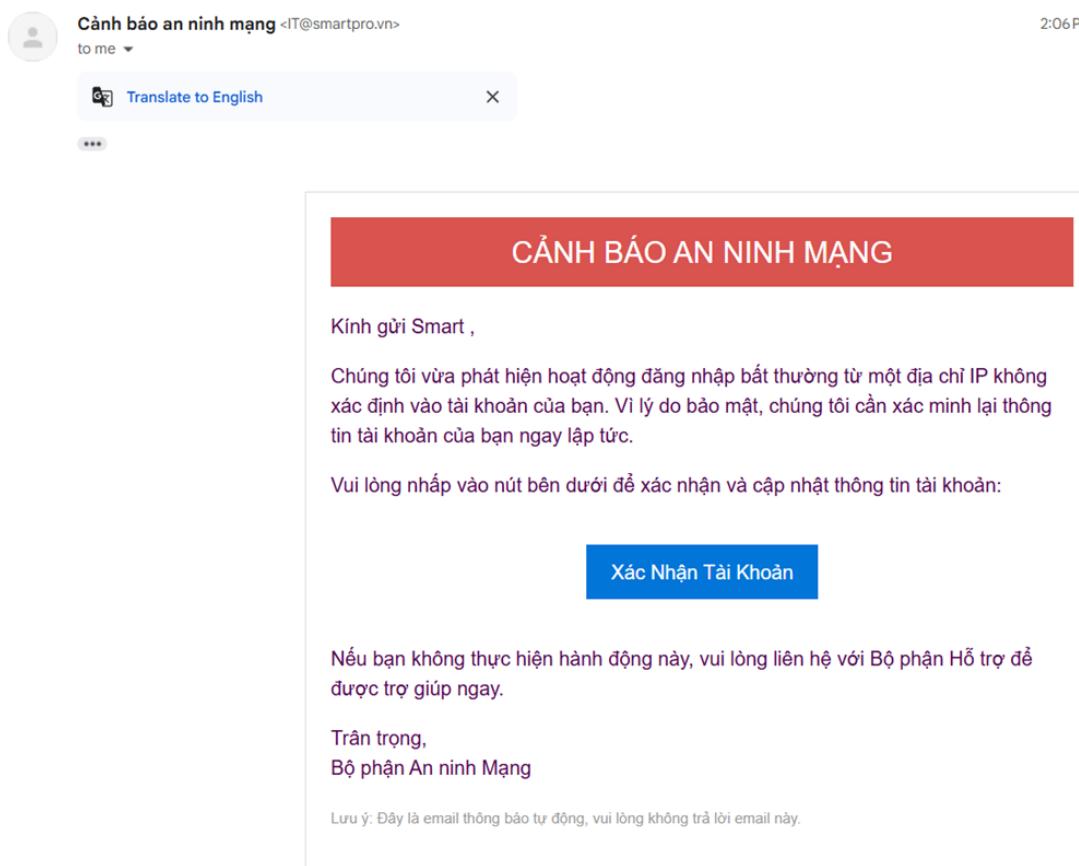
Groups:

x Genco1

Close

 Launch Campaign

- Sau khi điền xong thông tin, chọn Lauch Campaign để tiến hành gửi email phishing đến nạn nhân
- Email sẽ được gửi đến nạn nhân theo mẫu đã chỉnh ở phần Email Template
- Nạn nhân sẽ bấm vào xác nhận tài khoản và sẽ được đưa đến trang đăng nhập giả mạo



Cảnh báo an ninh mạng <IT@smartpro.vn>
to me 2:06 PM (1 hour ago) ☆ ↵ :

Translate to English X

...

CẢNH BÁO AN NINH MẠNG

Kính gửi Smart ,

Chúng tôi vừa phát hiện hoạt động đăng nhập bất thường từ một địa chỉ IP không xác định vào tài khoản của bạn. Vì lý do bảo mật, chúng tôi cần xác minh lại thông tin tài khoản của bạn ngay lập tức.

Vui lòng nhấp vào nút bên dưới để xác nhận và cập nhật thông tin tài khoản:

Xác Nhận Tài Khoản

Nếu bạn không thực hiện hành động này, vui lòng liên hệ với Bộ phận Hỗ trợ để được trợ giúp ngay.

Trân trọng,
Bộ phận An ninh Mạng

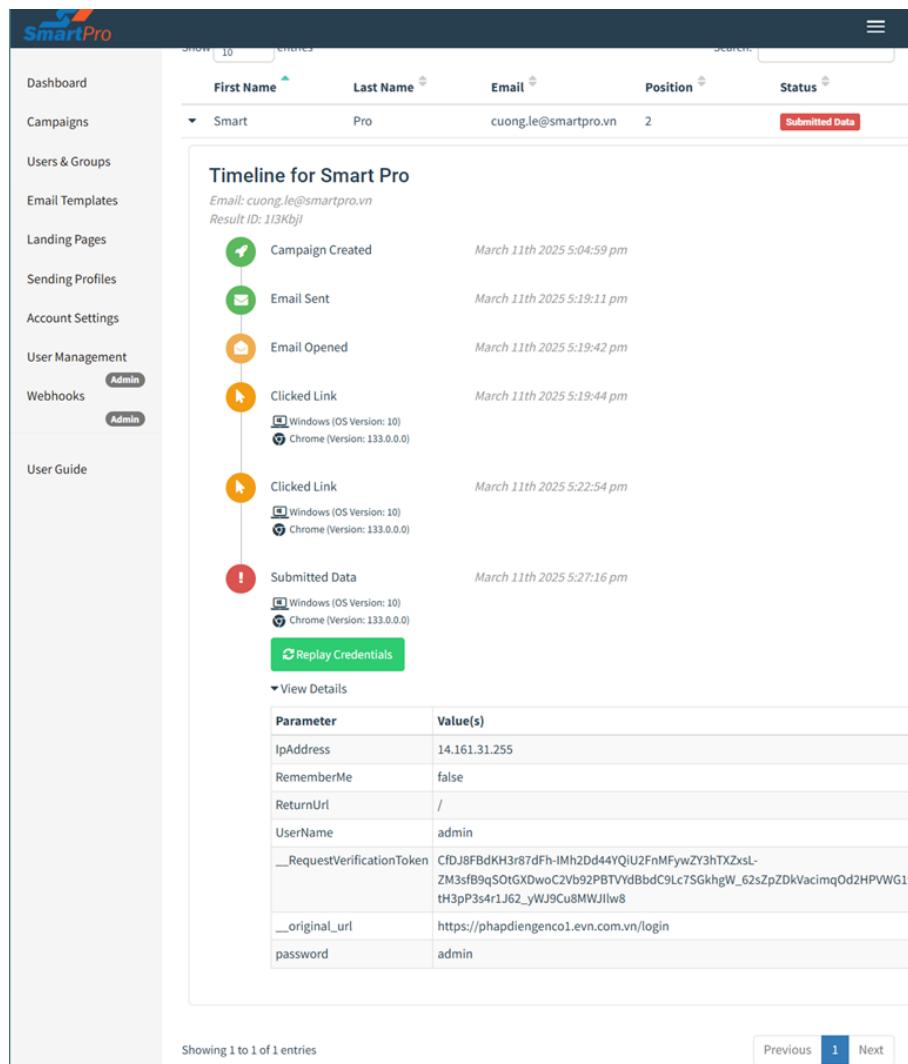
Lưu ý: Đây là email thông báo tự động, vui lòng không trả lời email này.

- Khi nạn nhân click vào “Xác nhận tài khoản” sẽ đưa nạn nhân đến trang web đăng nhập
- Bước 5: Xem Dashboard.

Dashboard sẽ hiển thị các giai đoạn như email được gửi, email được mở, nạn nhân đã click vào link chưa và cuối cùng là nạn nhân đã nhập dữ liệu chưa và có report mail là mail spam hay không.



- Phần details sẽ cho biết về hệ điều hành máy của nạn nhân, web browser và thời gian khi email được gửi, nạn nhân click và data nạn nhân nhập vào



Timeline for Smart Pro
 Email: cuong.le@smartpro.vn
 Result ID: 13Kbjl

Action	Date
Campaign Created	March 11th 2025 5:04:59 pm
Email Sent	March 11th 2025 5:19:11 pm
Email Opened	March 11th 2025 5:19:42 pm
Clicked Link	March 11th 2025 5:19:44 pm
Clicked Link	March 11th 2025 5:22:54 pm
Submitted Data	March 11th 2025 5:27:16 pm

Submitted Data

Parameter	Value(s)
IpAddress	14.161.31.255
RememberMe	false
ReturnUrl	/
UserName	admin
__RequestVerificationToken	CfDJ8FBdKH3r87dFh-IMh2Dd44YQiU2FnMFywZY3hTXxsL-ZM3sfB9qSOtGXwoC2Vb92PBTVYdBbdC9Lc7SGkhgW_62sZpZdkVacimqOd2HPVWG1w-th3pP3s4r1J62_yWJ9Cu8MWJlw8
__original_url	https://phapdiengenco1.evn.com.vn/login
password	admin