

স্ক্যানিং

আমরা এই অধ্যায়ে যে বিষয়গুলো নিয়ে আলোচনা করবো-

- স্ক্যানিং কি?
- কিভাবে স্ক্যানিং করা যায়?
- কিভাবে সিকিউয়ার করা যায়?

স্ক্যানিং কি?

রেকোননাইসেন্স এর পরের ধাপ হলো স্ক্যানিং। স্ক্যানিং হলো আপনি যে সিস্টেমকে হ্যাক করতে যাচ্ছেন বা যে সিস্টেমের দুর্বল দিকগুলো খুঁজে বের করতে যাচ্ছেন সেই সিস্টেমকে স্ক্যান করা। স্ক্যান করে সেই সিস্টেম এর কি কি ওপেন পোর্ট রয়েছে, কি কি সার্ভিস ওপেন রয়েছে, কি কি অপারেটিং সিস্টেম ব্যবহার করা হচ্ছে সেই গুলো সংগ্রহ করা।

কিভাবে স্ক্যানিং করা যায়?

১. পোর্ট স্ক্যানিং

২. নেটওয়ার্ক স্ক্যানিং

৩. ভুলনোরাবিলিটিজ স্ক্যানিং

১. পোর্ট স্ক্যানিং

পোর্ট স্ক্যানিং হলো যে পোর্টগুলো ওপেন আছে সেই পোর্টগুলো বের করা। পোর্ট স্ক্যানিং করার জন্য বিভিন্ন ধরনের টুল রয়েছে। তাদের মধ্যে উল্লেখযোগ্য হলো- nmap

চলুন Nmap নিয়ে বিস্তারিত জানার চেষ্টা করি-

পোর্ট স্ক্যানিং এর জন্য আমরা কিভাবে nmap ইন্সটল করবো?

ধাপ-০১: nmap সফটওয়্যারটি প্রথমে ডাউনলোড করতে হবে এই ওয়েবসাইট থেকে-

Download the Free Nmap Security Scanner

https://nmap.org/download.html

NMAP.ORG

Nmap Security Scanner

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists

- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools

- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation

Your Ports are Showing!
What does your security say about you?

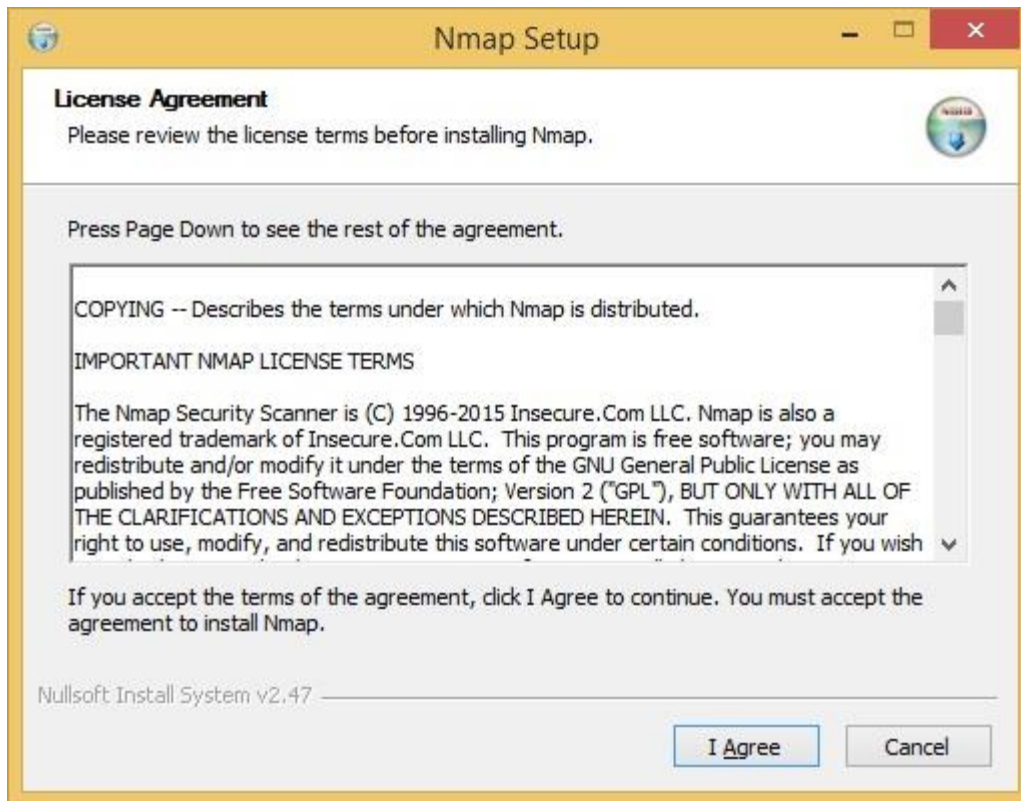
Intro	Reference Guide	Book	Install Guide
Download	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies			In the News

Downloading Nmap

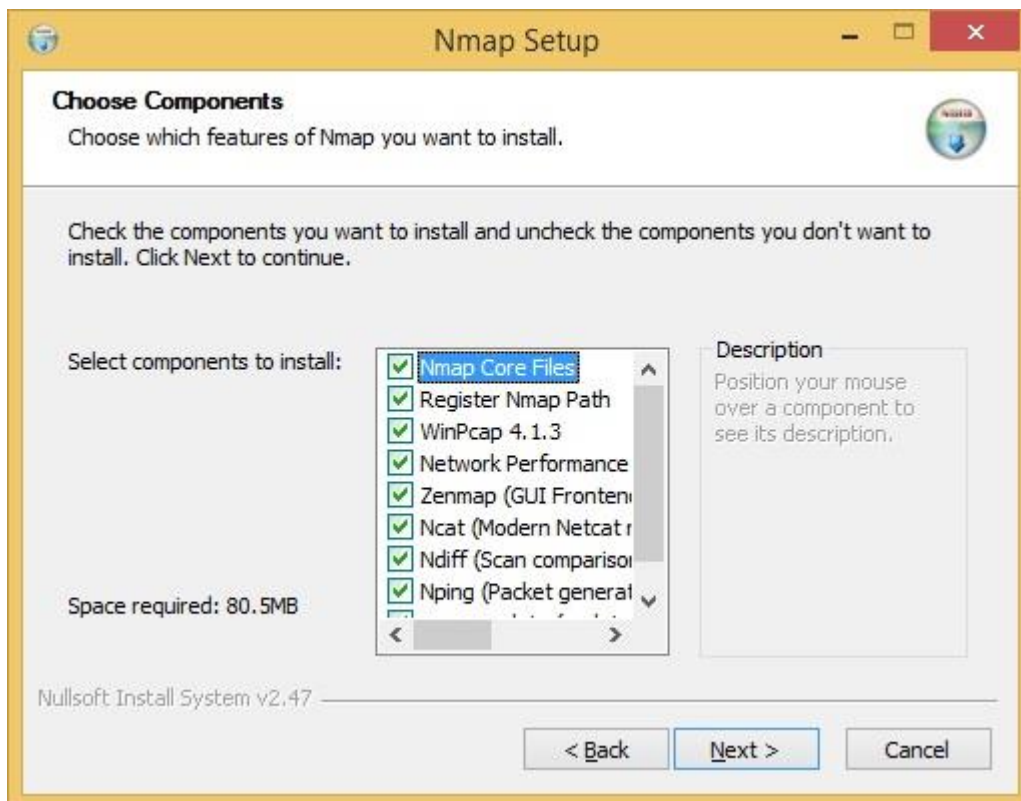
Nmap and Zenmap (the graphical front end) are available in several versions and formats. Recent source releases and binary packages are described below. Older version (and sometimes newer test releases) are available from the [dist directory](#) (and really old ones are in [dist-old](#)). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the [sigs directory](#) ([verification instructions](#)). Before downloading, be sure to read the relevant sections for your platform from the [Nmap Install Guide](#). The most important changes (features, bugfixes, etc) in each Nmap version are described in the [Changelog](#). Using Nmap is covered in the [Reference Guide](#), and don't forget to read the other [available documentation](#), particularly the new book [Nmap Network Scanning!](#)

Nmap users are encouraged to subscribe to the [Nmap-hackers](#) mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

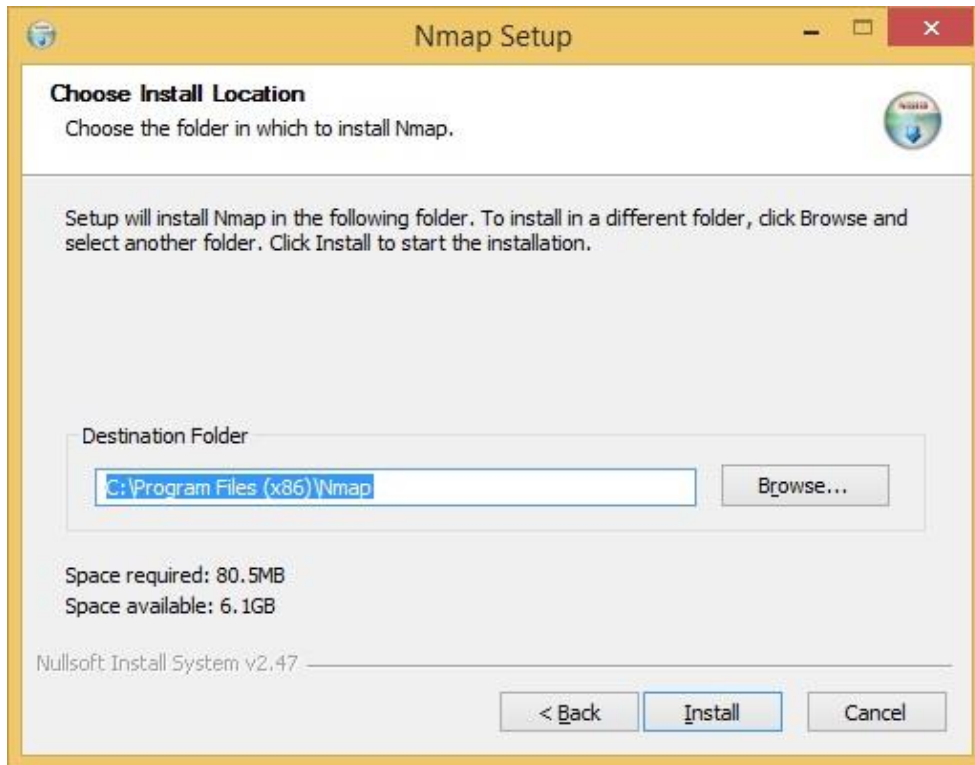
ধাপ-০২: তারপর .exe রান করে ইন্সটল করতে হবে।



ধাপ-০৩: যে কম্পোনেন্টস গুলো ইন্সটল করবেন সেইগুলো সিলেক্ট করতে হবে৷



ধাপ-০৪: ইন্সটলেশন ফোল্ডার লকেশন সিলেক্ট করে দিতে হবে।

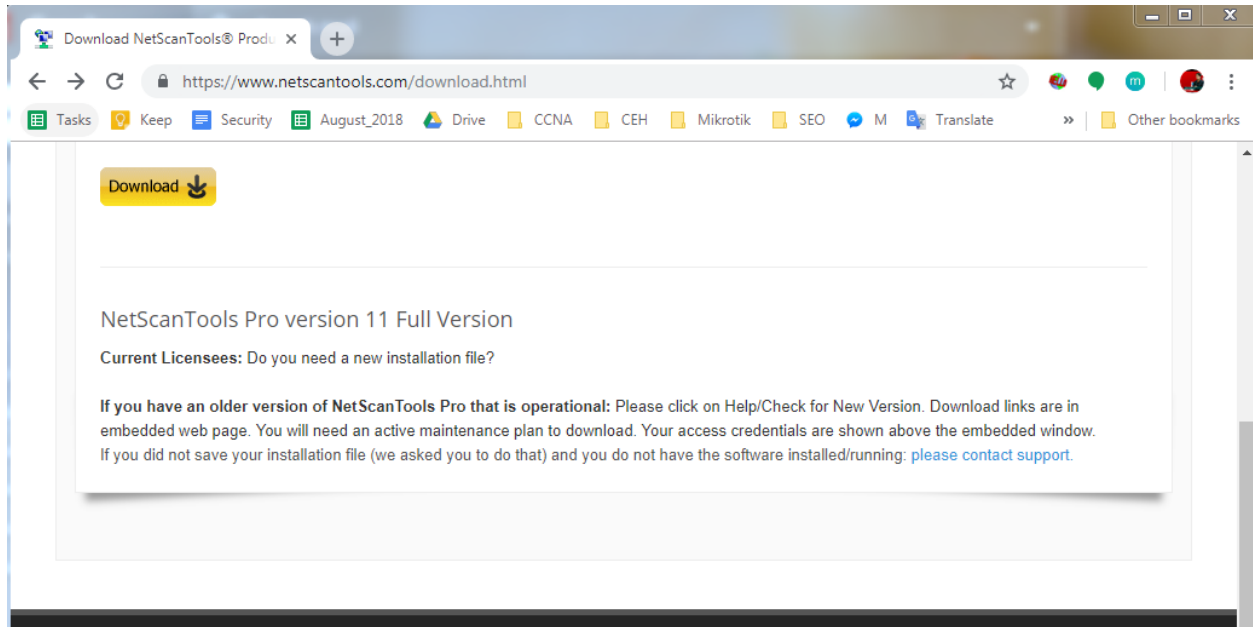


২. নেটওয়ার্ক স্ক্যানিং

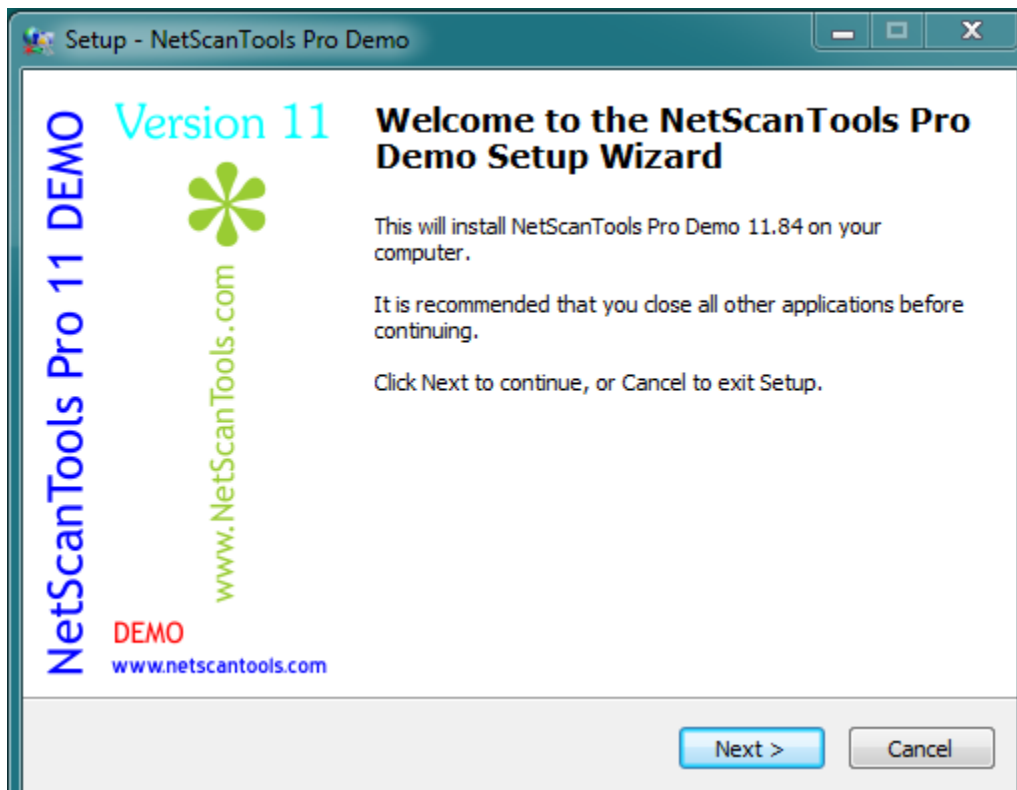
নেটওয়ার্ক স্ক্যানিং হলো নেটওয়ার্কে কি কি পিং করে রিপোর্ট পাওয়া যায় এবং এভাবে লেভেল কি কি আইপি রয়েছে তা খুঁজে বের করা। নেটওয়ার্ক স্ক্যানিং করার জন্যও বিভিন্ন ধরনের টুল রয়েছে। তাদের মধ্যে উল্লেখযোগ্য হলো- Nmap Tools pro

চলুন দেখি কিভাবে NetScan Tools pro টি ব্যবহার করা যায় ?

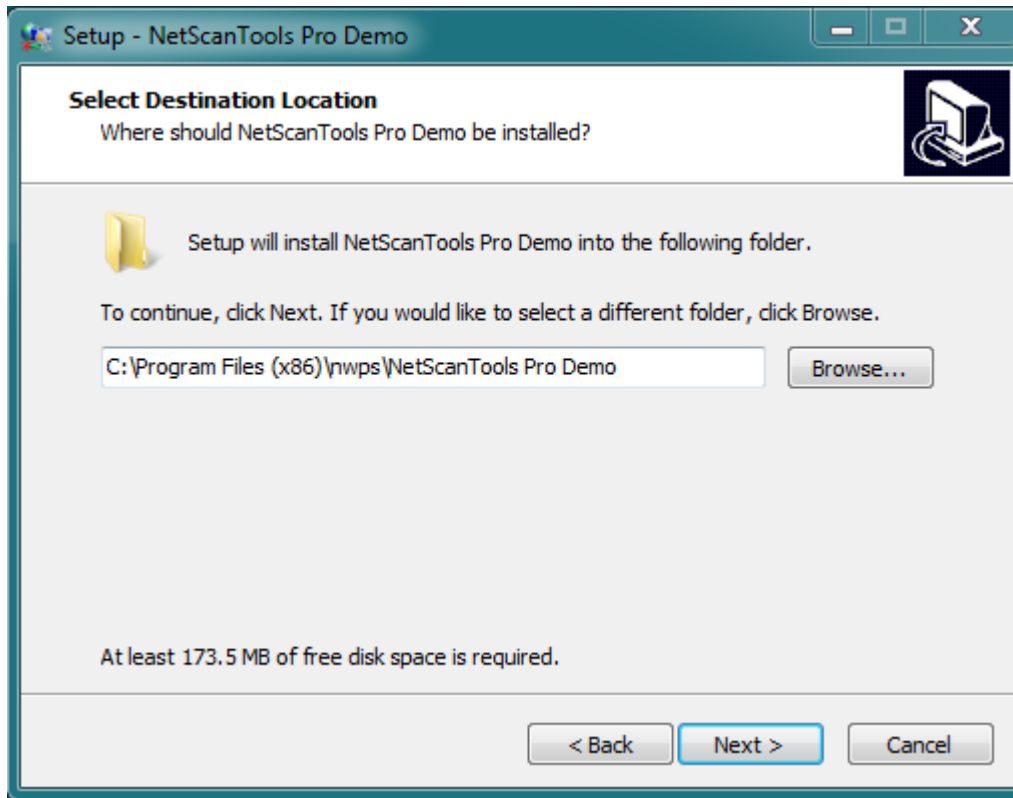
ধাপ-০১: এই টুলসটি আমরা প্রথমে ডাউলোড করে নিতে পরি এই সাইট (netscantools.com)থেকে।



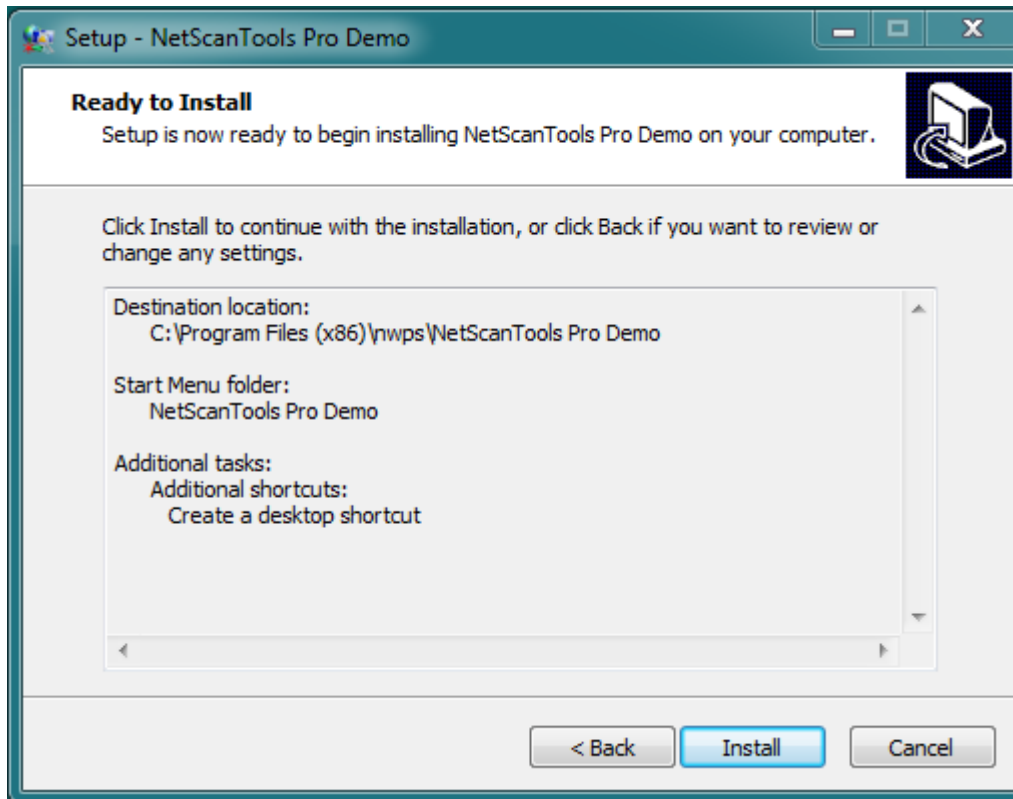
ধাপ-০২: এই টুলসটি ইন্সটল করতে হবে।



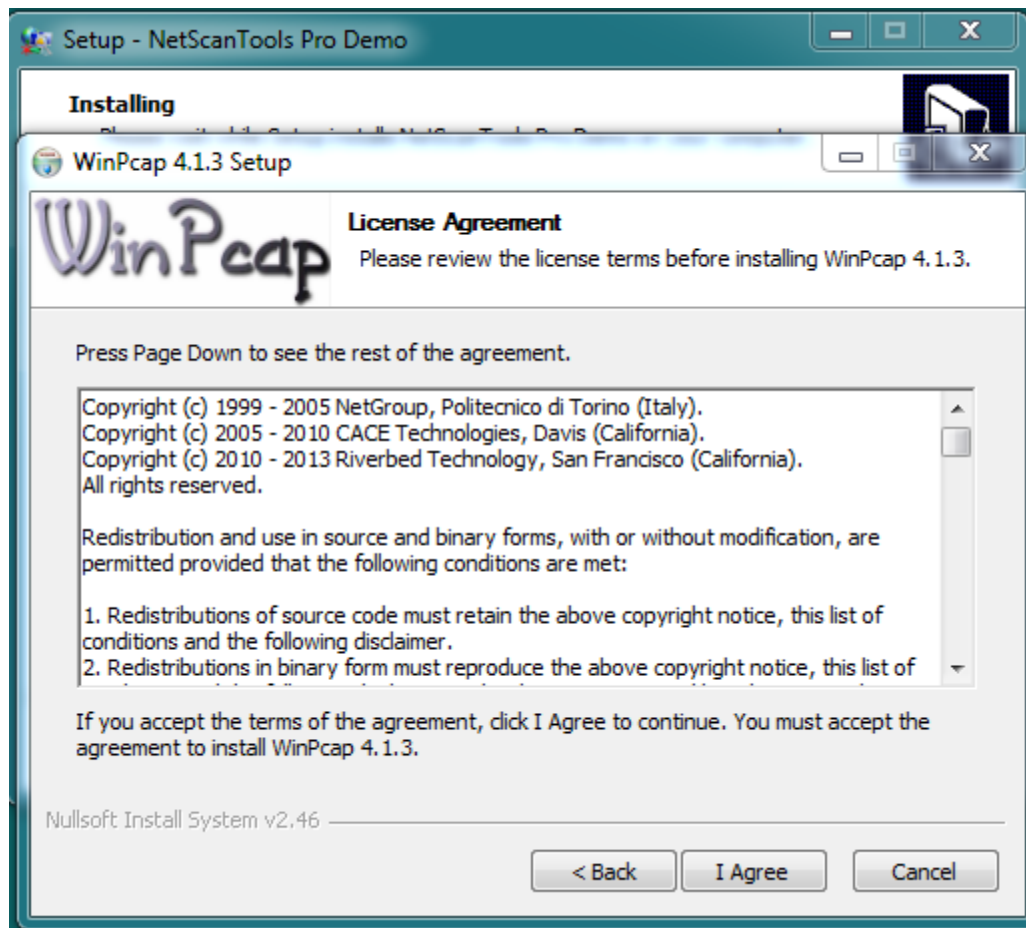
ধাপ-০৩: যে লকেশনে ইন্সটল করতে ইচ্ছুক সেই লকেশনটি সিলেক্ট করে দিতে হবে।



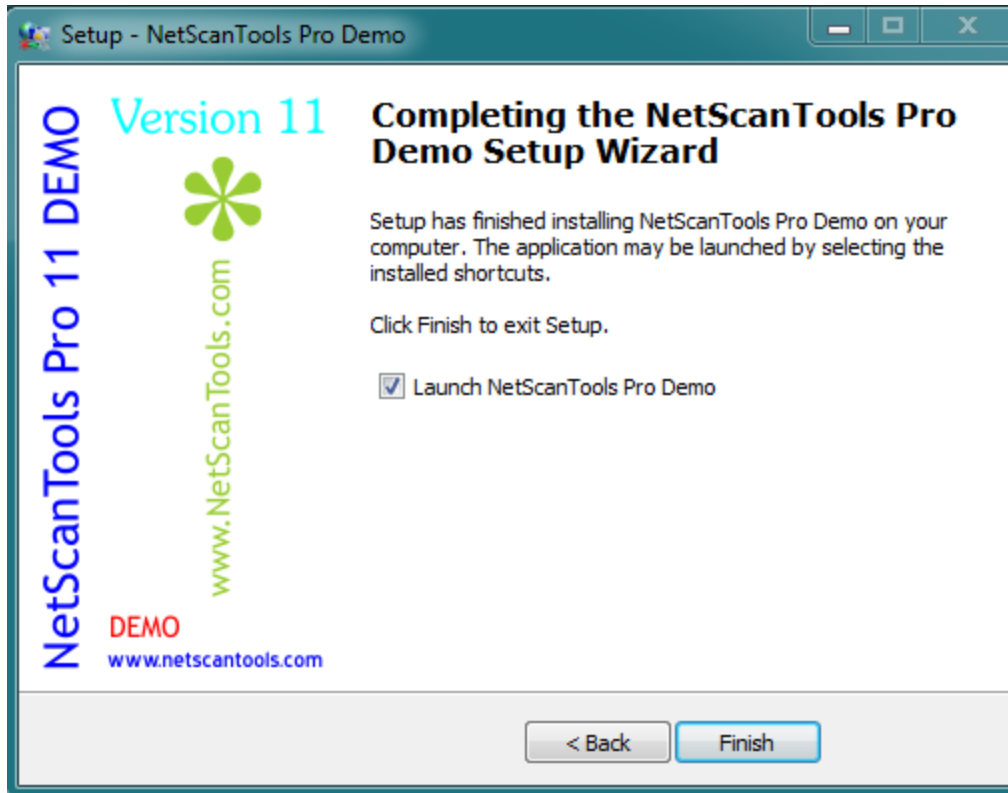
ধাপ-০৪: ইন্সটলে ক্লিক করলেই ইন্সটল শুরু হয়ে যাবে।



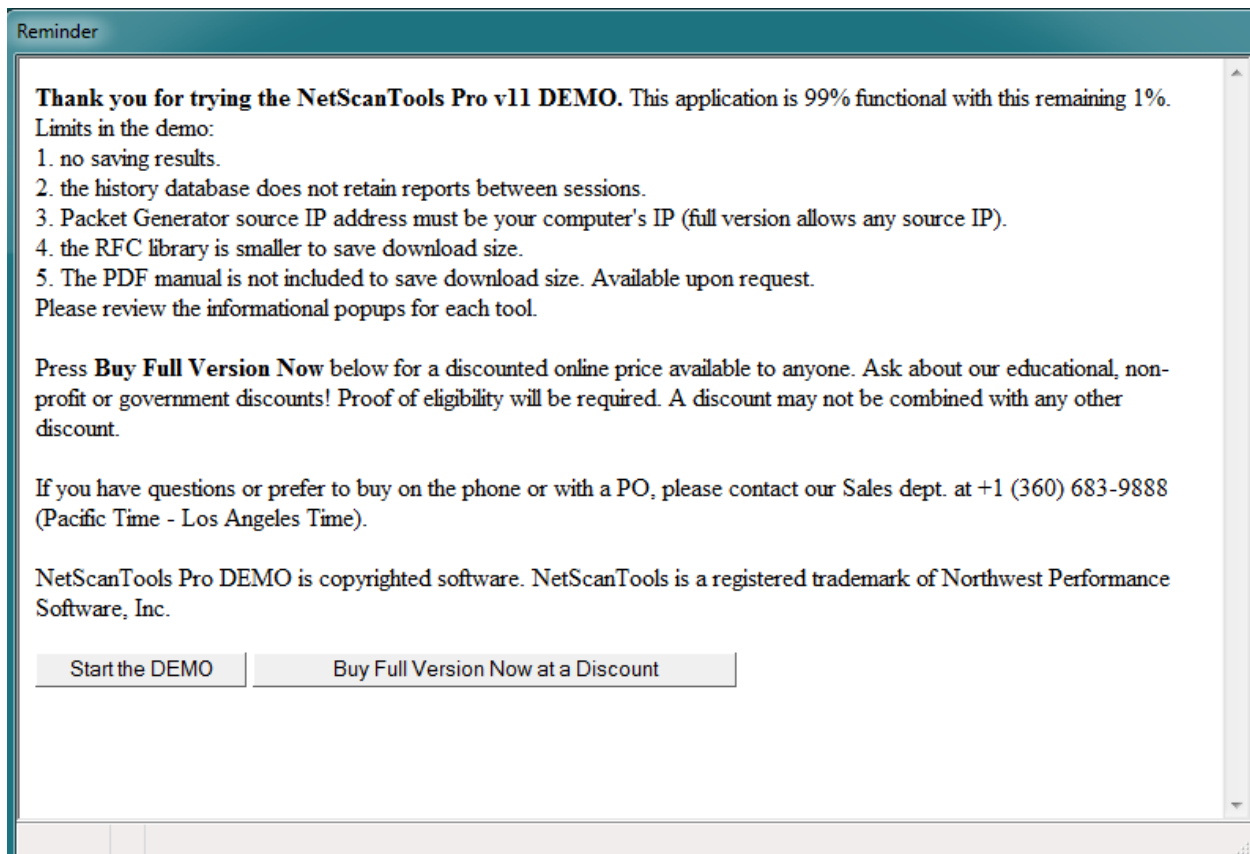
ধাপ-০৫: এই সফটওয়্যারটি পূর্বশর্ত তাই ইন্সটল ডায়ালগ বক্স আসলে ইন্সটল করতে হবে।



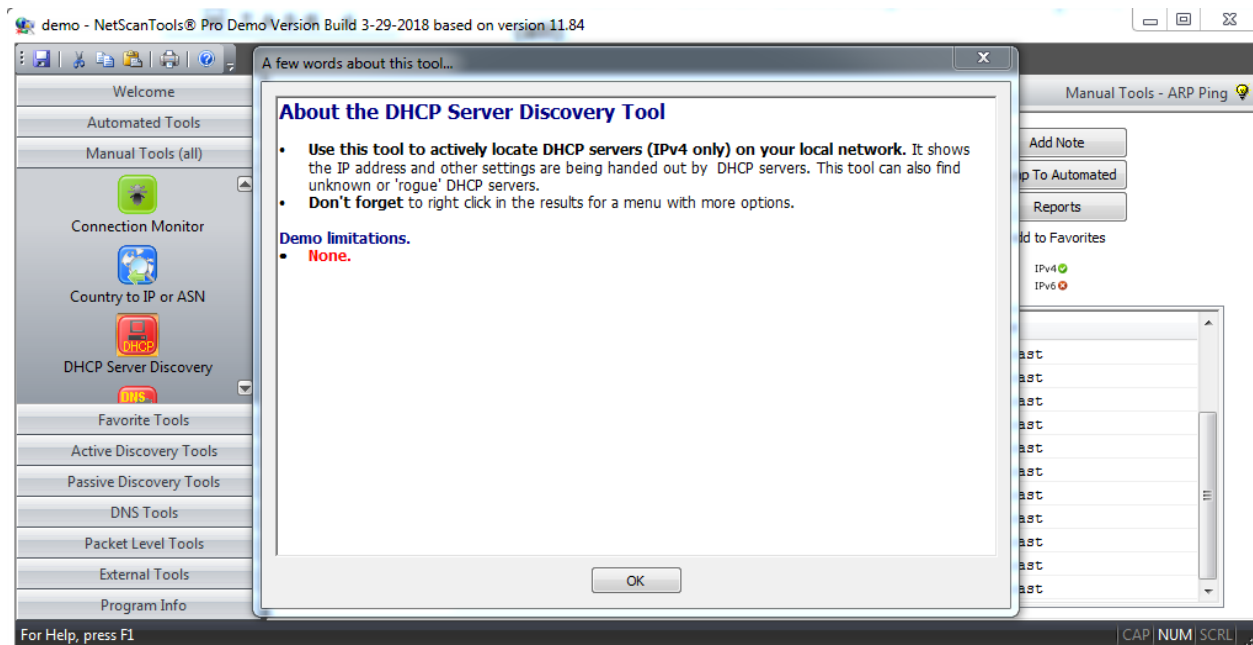
ধাপ-০৬: তারপর টুলসটি ওপেন করতে হবে।



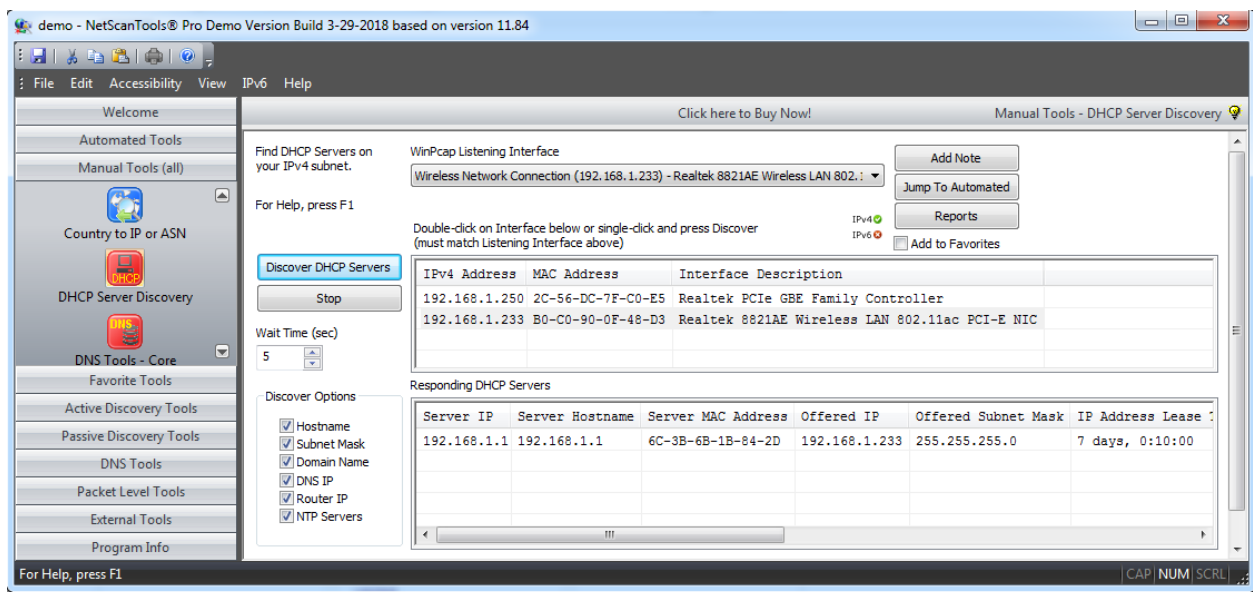
ধাপ-০৭: ডেমো হিসেবে শুরু করতে হবে।



ধাপ-০৮: আমরা যদি চাই এই নেটওয়ার্কে কোন ডিএইচসিপি সার্ভার আছে কি না তা চেক করবো, সাথে সাথে কোন পিসি কোন আইপি ব্যবহার করছে তা চেক করবো। তাহলে, আমরা ম্যানুয়াল টুলস থেকে ডিএইচসিপি সার্ভার ডিসকভারীতে ক্লিক করবো।



ধাপ-০৯: ডিসকভার ডিএইচসিপি সার্ভার এ ক্লিক করলেই নীচের মতো আউটপুট দেখা যাবে। অর্থাৎ কে কোন আইপি ব্যবহার করছে, কোন পিসির ম্যাক এড্রেস কত ইত্যাদি।



৩. ভুলনোরাবিলিটিজ স্ক্যানিং

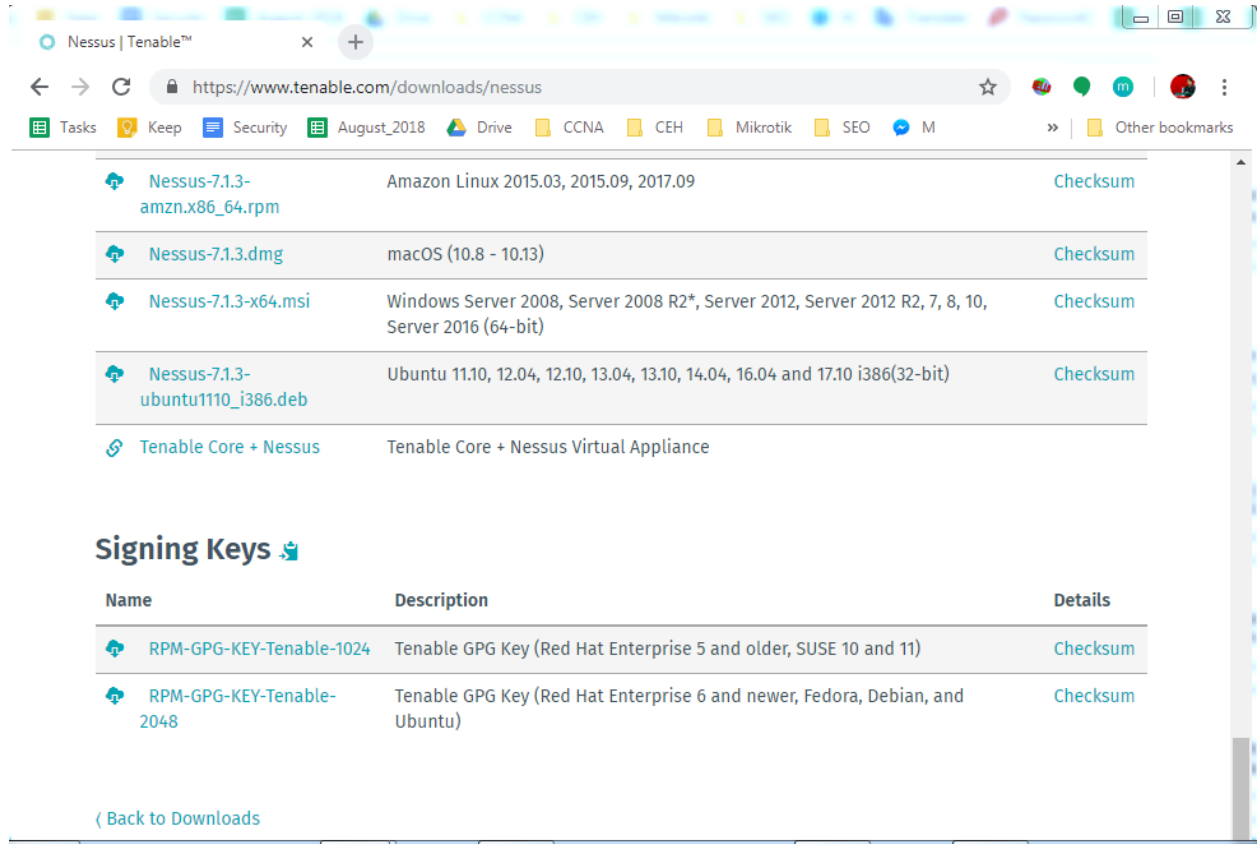
ভুলনোরাবিলিটিজ স্ক্যানিং হলো কোন একটি সিস্টেম অথবা নেটওয়ার্কের কি কি সিকিউরিটি হোল রয়েছে সেইগুলো স্ক্যান করে বের করা।

ভুলনোরাবিলিটিজ স্ক্যানিং এর জন্য ব্যবহৃত টুলস হলো-Nessus

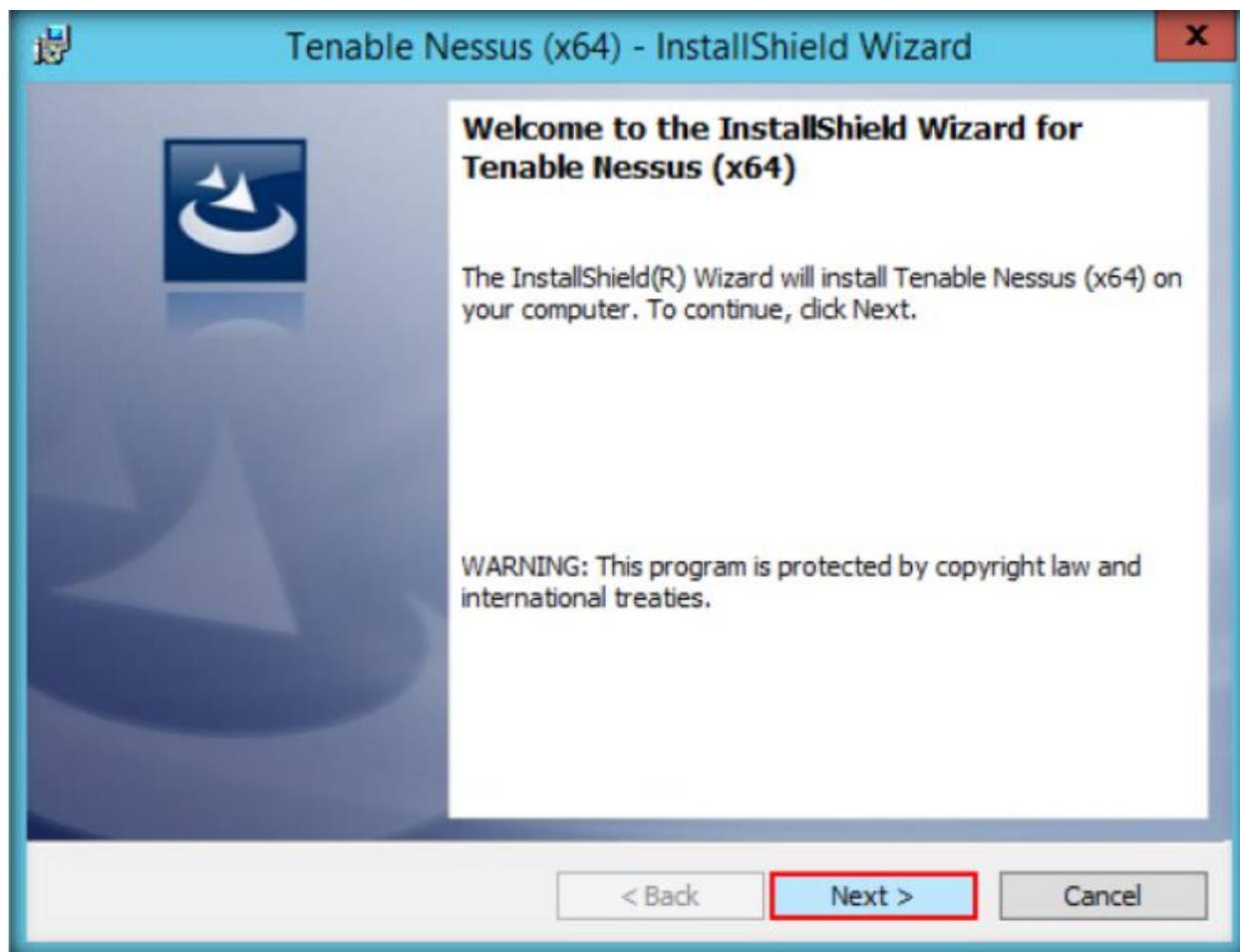
কিভাবে Nessus ইন্সটল এবং কনফিগার করবেন ?

Nessus ইন্সটল করার সময় যে ধাপগুলো অনুসরণ করতে হবে।

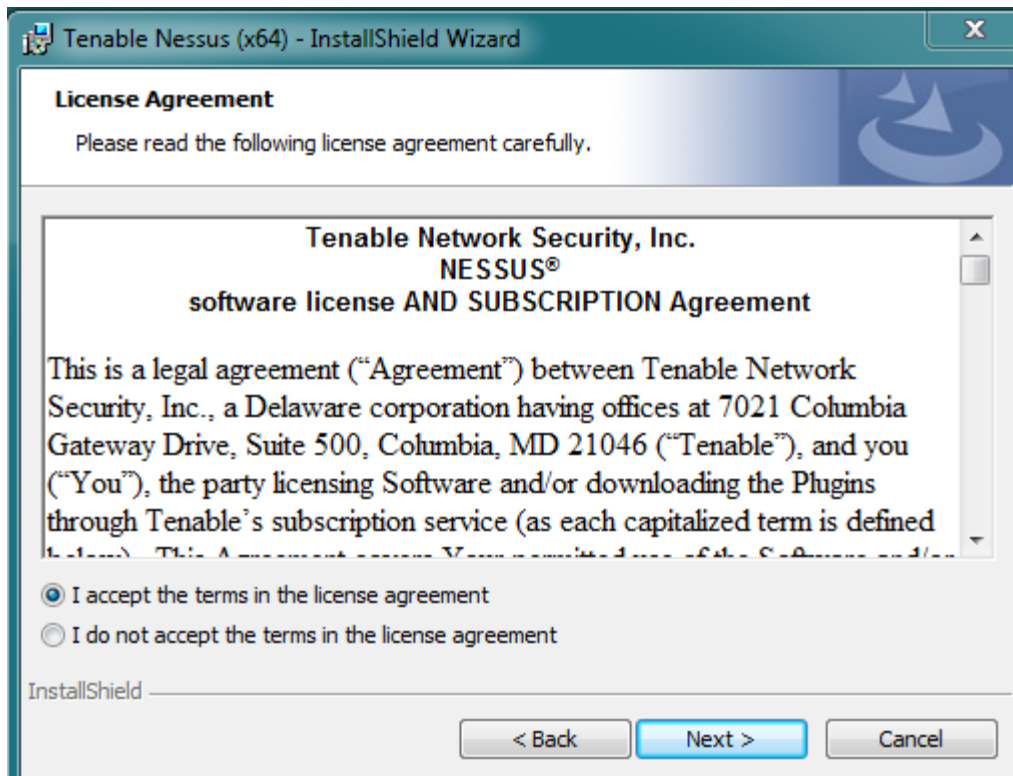
ধাপ-০১: প্রথমে (nessus) টুলসটি এই লিংক(<https://www.tenable.com/downloads/nessus>) থেকে ডাউনলোড করতে হবে।



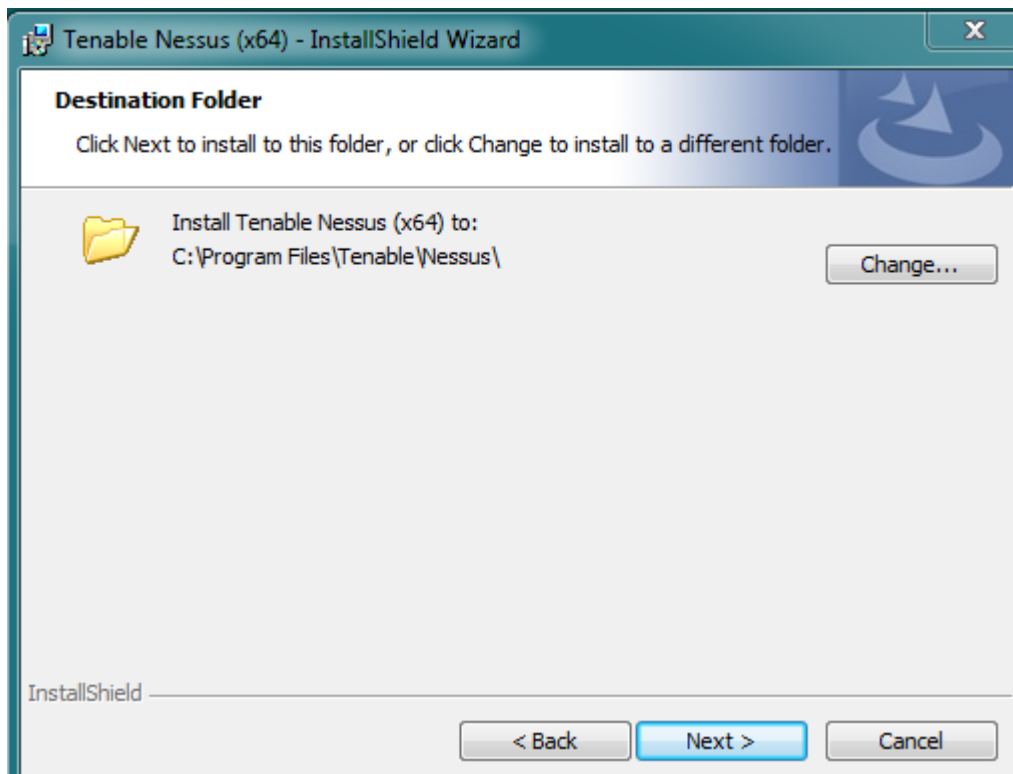
ধাপ-০২: এই টুলটি ইন্সটল করতে হবে।



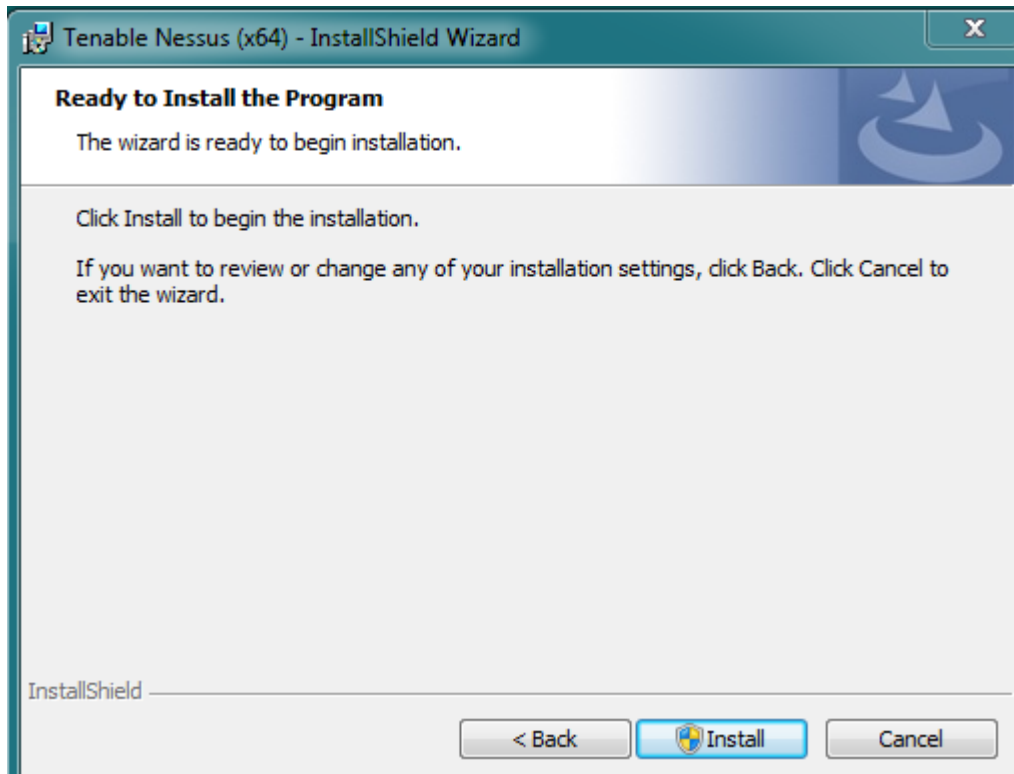
ধাপ-০৩: একসেপ্ট সিলেক্ট করে নেক্সট এ ক্লিক করতে হবে।



ধাপ-০৪: ইন্সটলেশন ফোল্ডার সিলেক্ট করে দিতে হবে।



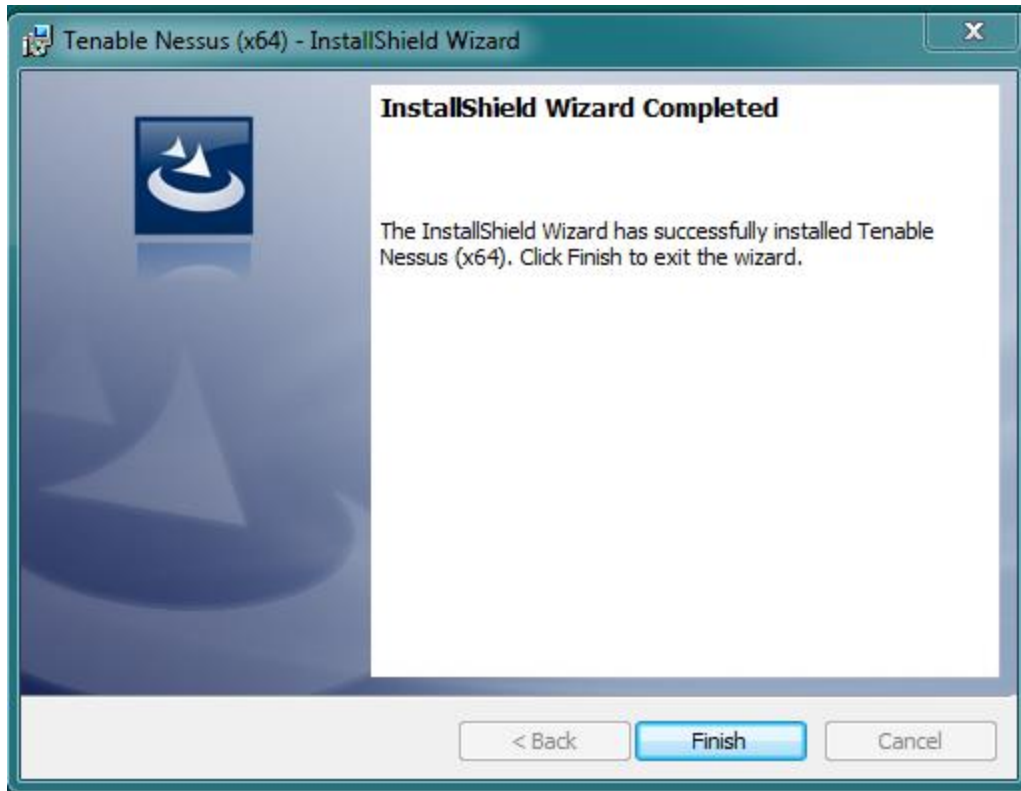
ধাপ-০৫: ইন্সটল এ ক্লিক করতে হবে।



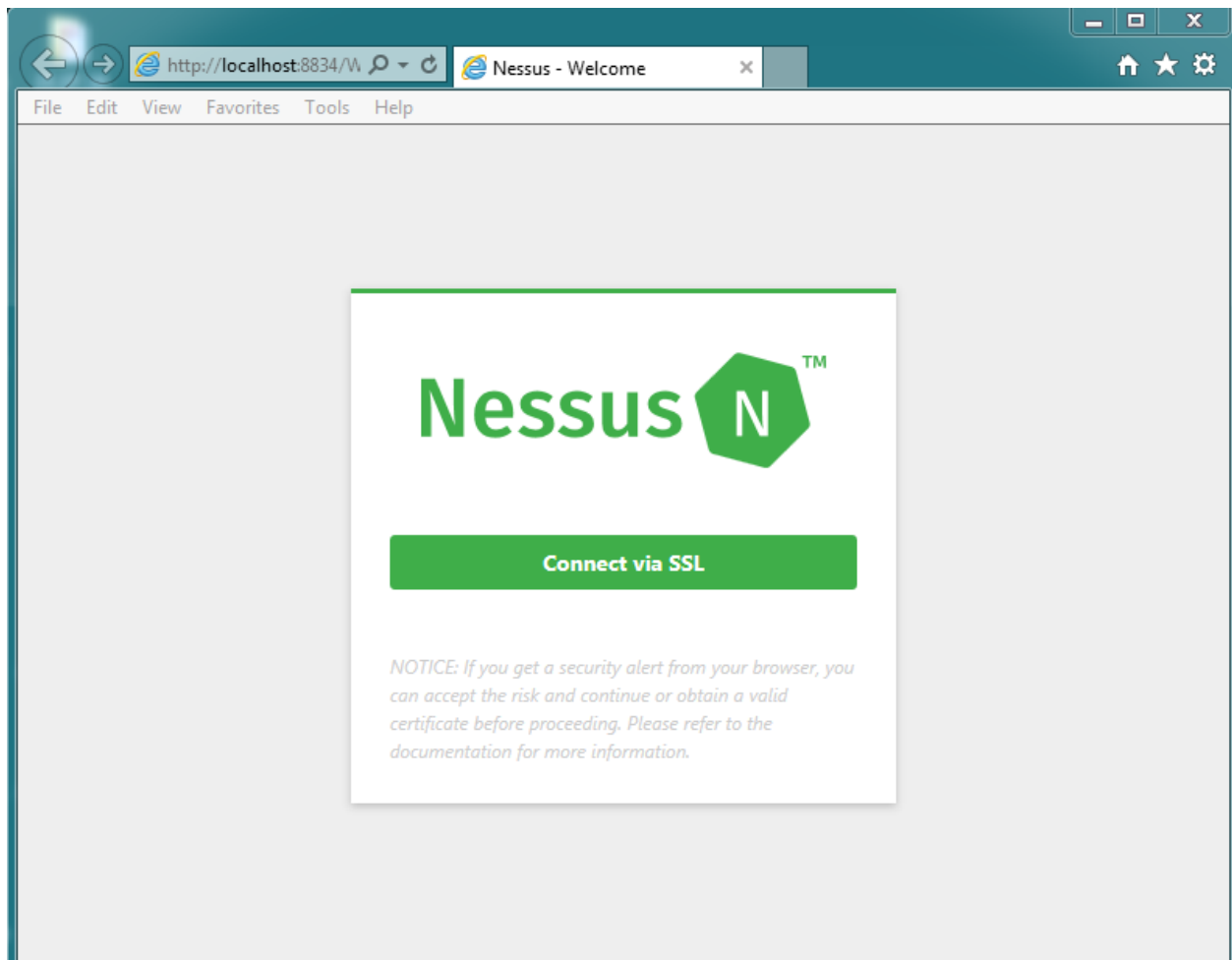
ধাপ-০৬: এই এ্যাপ্লিকেশনটি পূর্বশর্ত তাই ইন্সটল করতে হবে।



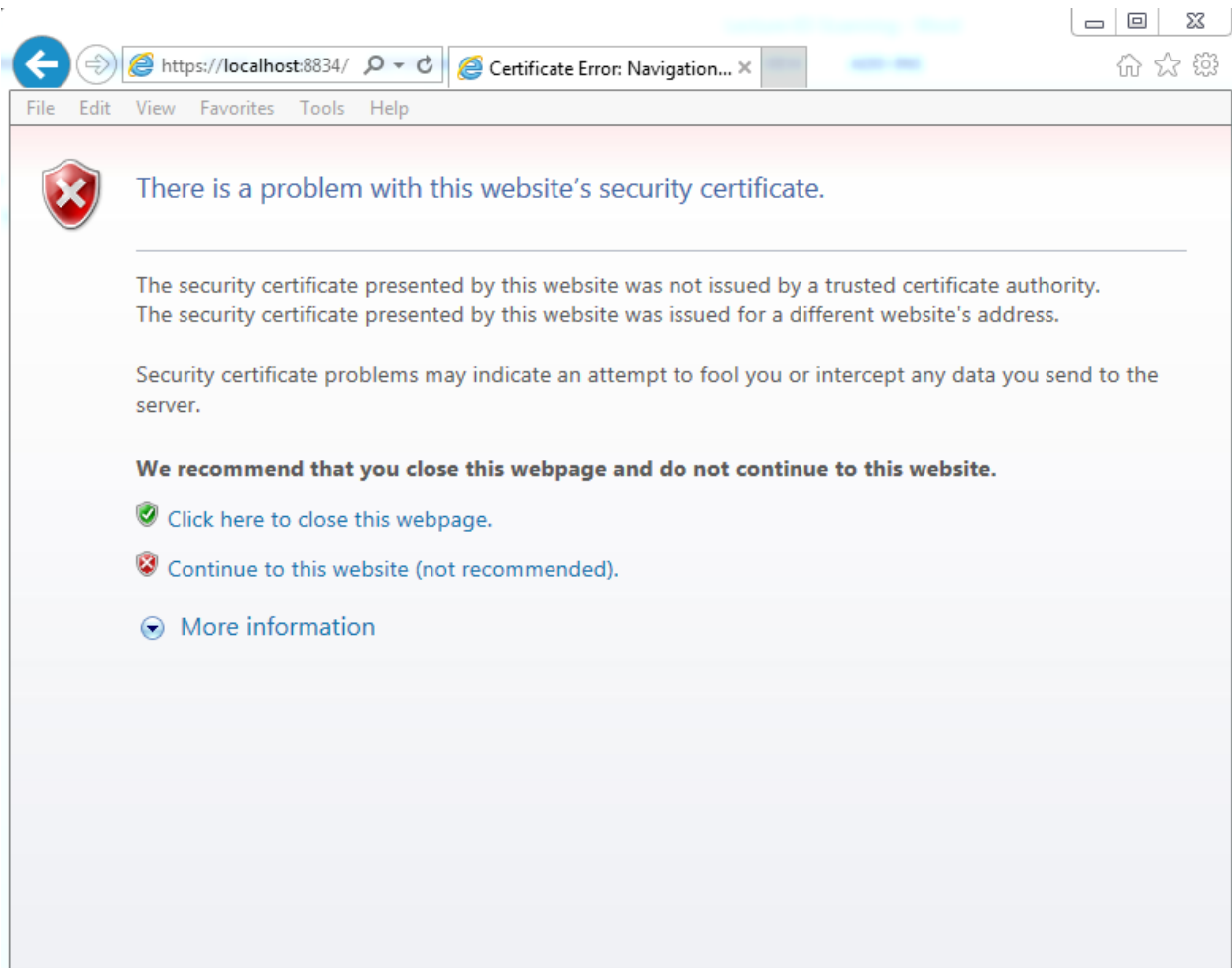
ধাপ-০৭: সবশেষে ফিনিস এ ক্লিক করলেই ইন্সটলেশন শেষ হবে।



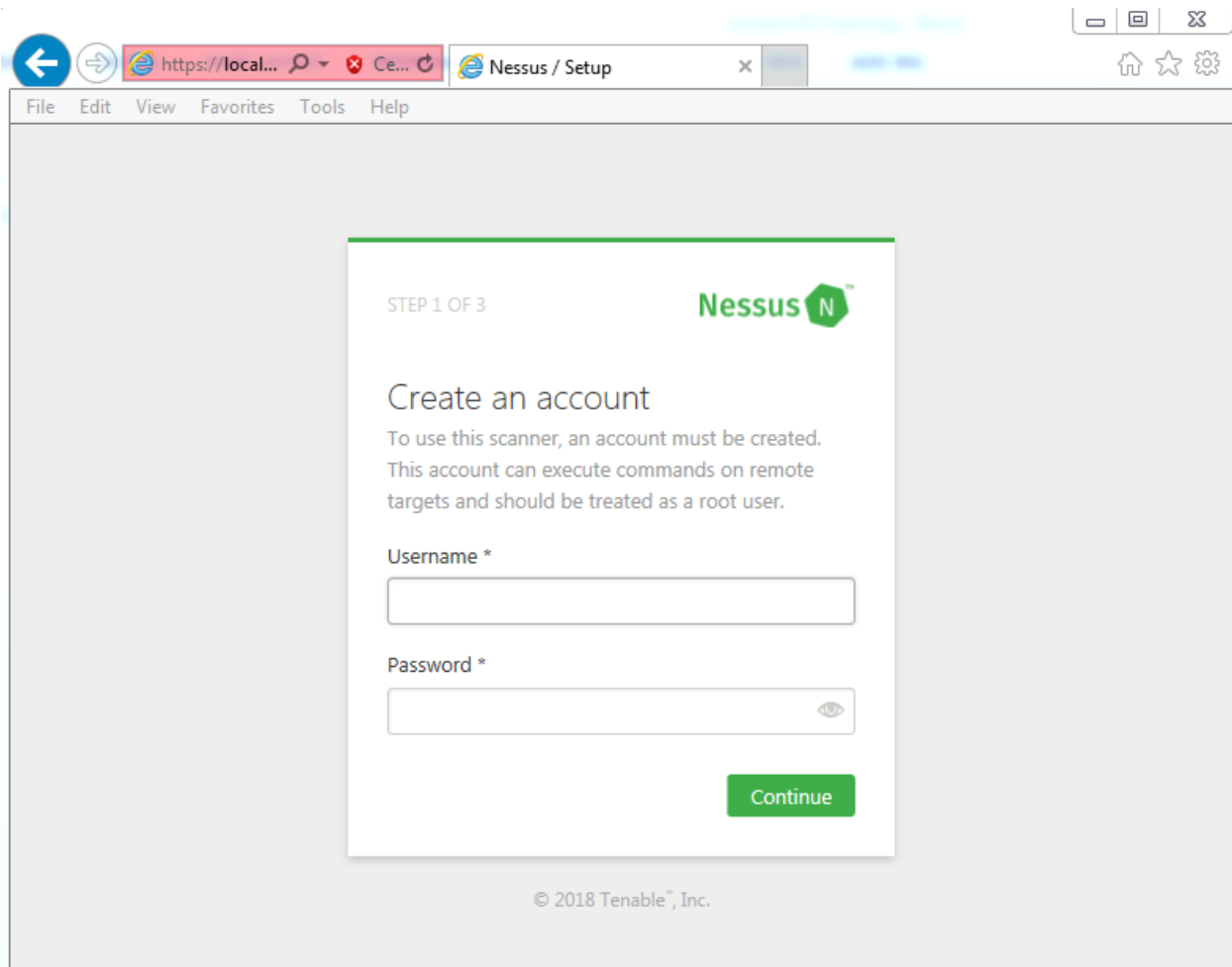
ধাপ-০৮: তারপর ব্রাউজারের মাধ্যমে কনফিগার করতে হবে।



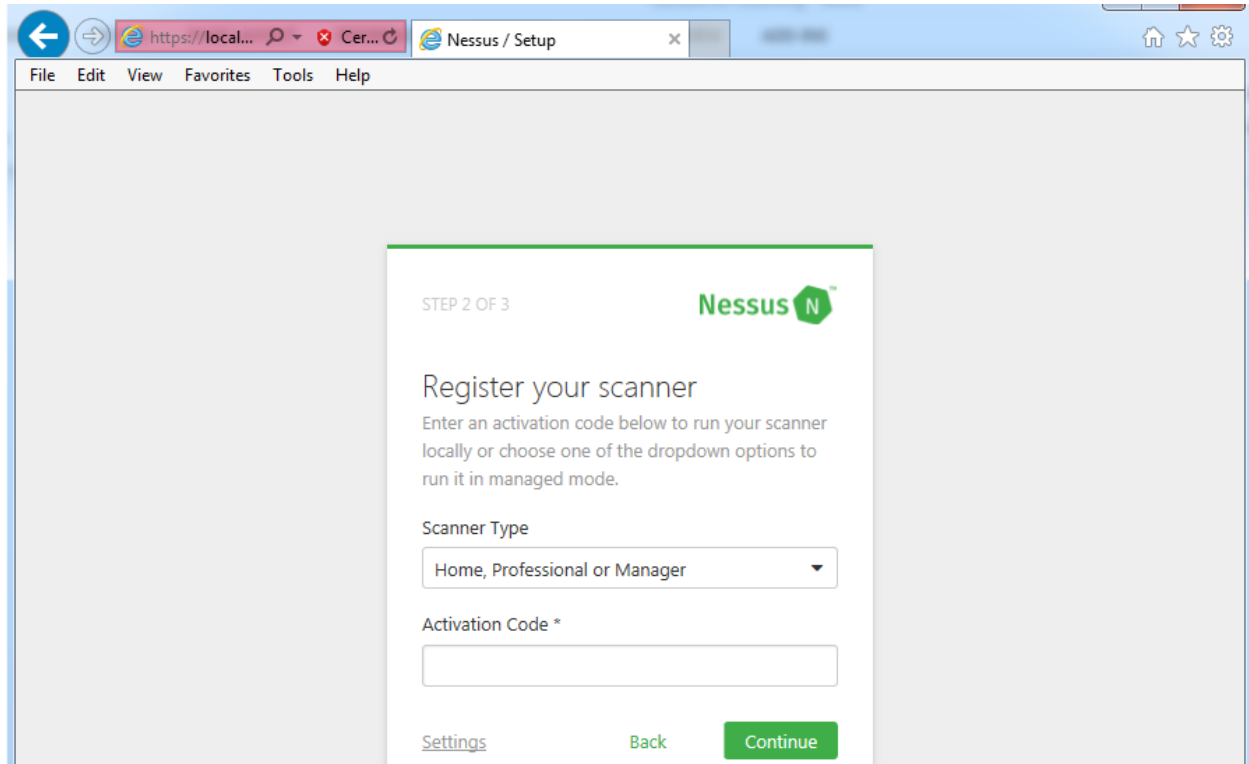
ধাপ-০৯: connect via SSL এ ক্লিক করলে এই ধরনের একটি ম্যাসেজ আসবে, তারপর Continue the website এ ক্লিক করতে হবে।



ধাপ-১০: এখানে একটি নাম এবং পাসওয়ার্ড দিয়ে রেজিস্ট্রেশন করতে হবে।



ধাপ-১১: তারপর Continue এ ক্লিক করলেই একটি একটিভেশন কোড দেওয়ার জন্য বলা হবে।



ধাপ-১২: একটিভেশন কোড সংগ্রহ করা জন্য এই লিংকে

(<https://www.tenable.com/products/nessus-home>) রেজিস্ট্রেশন করতে হবে।

Nessus Home | Tenable™

https://www.tenable.com/products/nessus-home

Tasks Keep Security August_2018 Drive CCNA CEH Mikrotik SEO M Other bookmarks

tenable Cyber Exposure Products Solutions Services Company Partners Blog Login Free Trial Buy Now

Nessus® Home allows you to scan your personal home network (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Home does not provide access to support, allow you to perform compliance checks or content audits, or allow you to use the Nessus virtual appliance. If you require support and these [additional features](#), please purchase a [Nessus](#) subscription.

Nessus Home is available for personal use in a home environment only. It is not for use by any commercial organization.

Register for an Activation Code

First Name * Last Name *

titas sarker

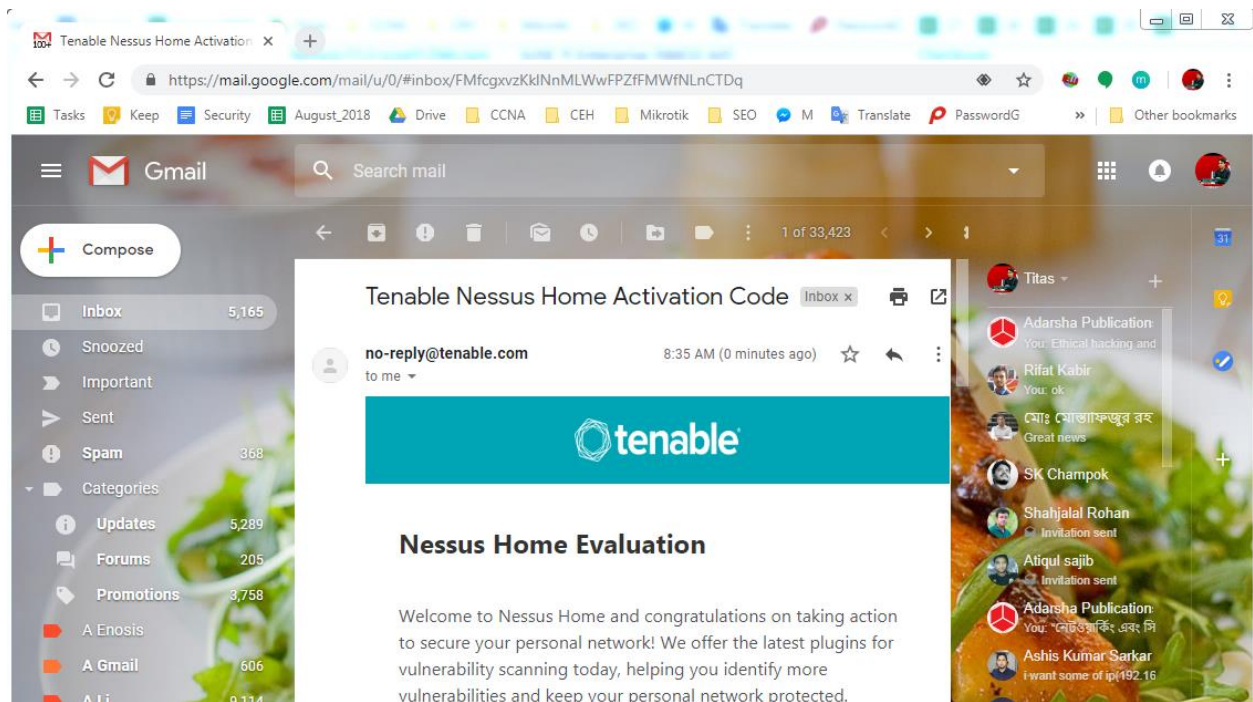
Email *

titasce@gmail.com

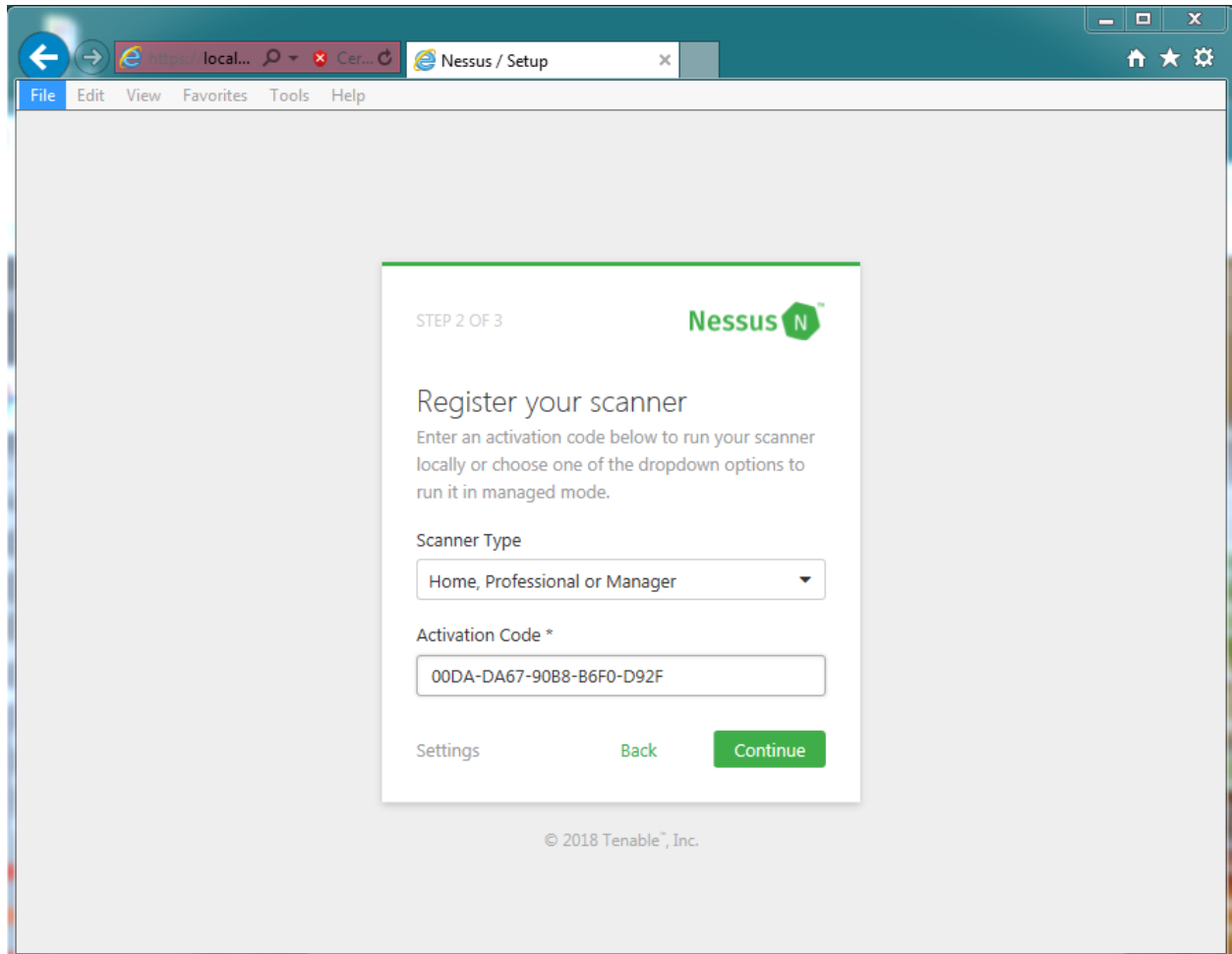
☐ Check to receive updates from Tenable

Register

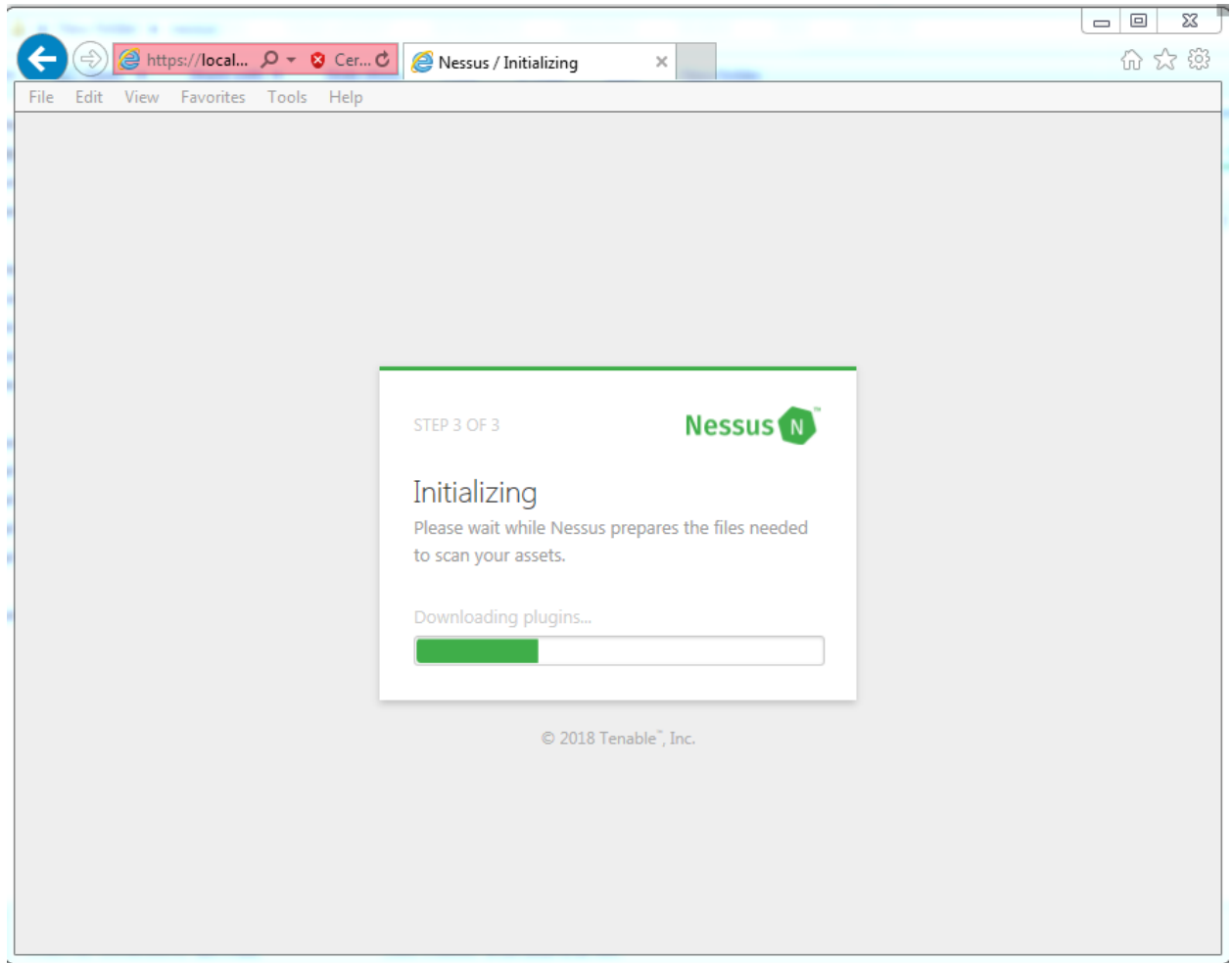
ধাপ-১৩: একটি একটিভেশন কোড ইমেইল করবে।



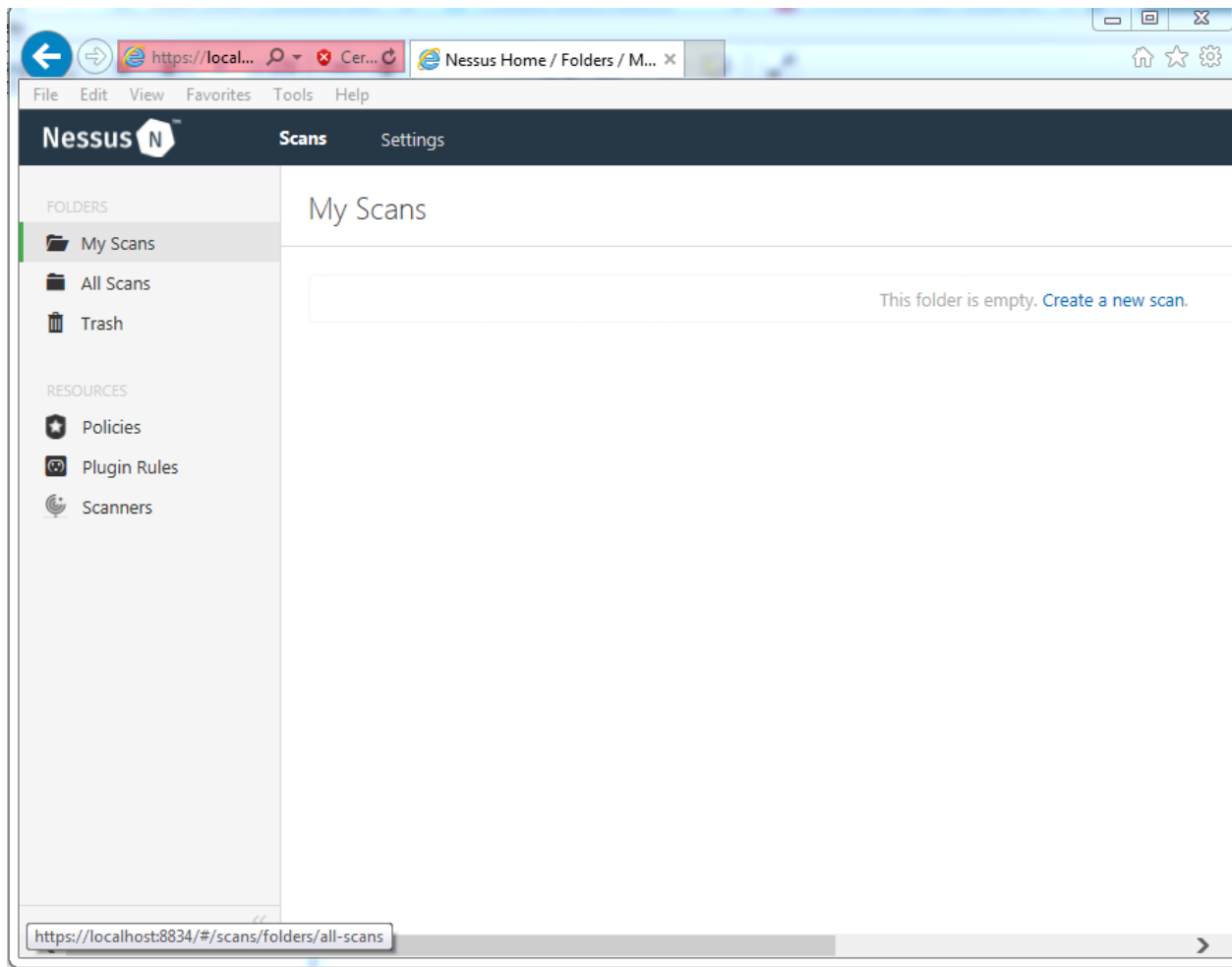
ধাপ-১৪: তারপর এই একটিভেশন কোডটি রেজিস্ট্রেশন বক্সে দিতে হবে।



ধাপ-১৫: কোডটি দেওয়ার পর ইনিশিয়ালাইজেশনের জন্য অনেকটা সময় অপেক্ষা করতে হবে।



ধাপ-১৬: এখন আপনি যে বিষয়টি স্ক্যান করতে চান সেইটি সিলেক্ট করে করে স্ক্যান করতে পারেন।



কিভাবে সিকিউয়ার করা যায়?

- মাল্টিলেয়ার এ একাধিক ফায়ারওয়াল ব্যবহার করতে হবে।
- এনক্রিপ্ট করে সকল ট্রাফিক ট্রান্সফার করতে হবে।
- সকল অপ্রয়োজনীয় পোর্টগুলো বন্ধ রাখতে হবে।
- আইপি এবং ম্যাক বাইন্ডিং সার্ভিস স্থাপন করতে হবে।