**Nmap**

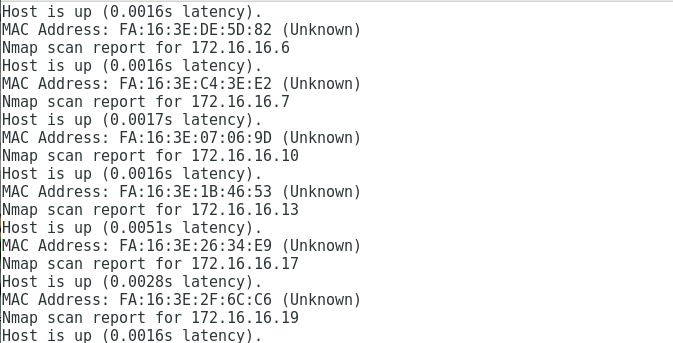
1. Installing nmap

$ sudo yum install nmap (Redhat/Fedora)

$ sudo apt-get install nmap (Ubuntu/Debian)

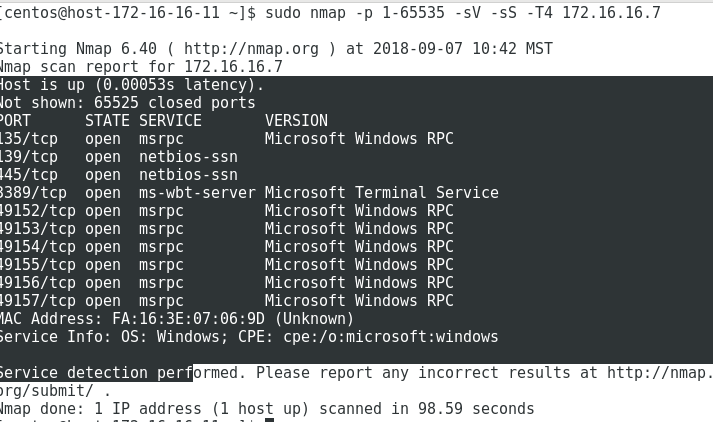
2. Checking the devices on your network responding to ping scan.

$ sudo nmap -sP 192.168.1.0/24



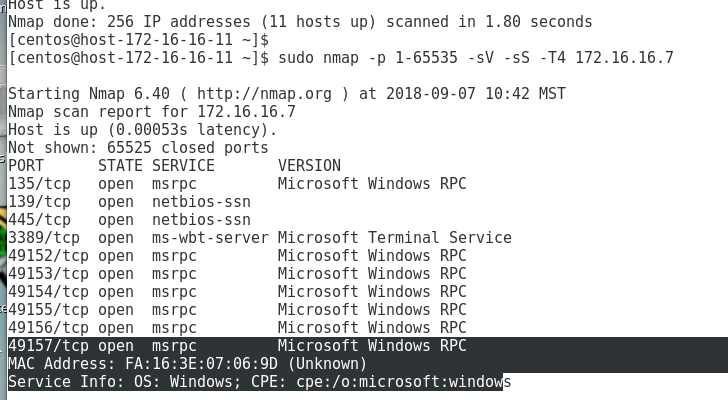
3. Full TCP port scan using with service version detection.

$ sudo nmap -p 1-65535 -sV -sS -T4 target



4. OS and version detection + traceroute and scripts against target services

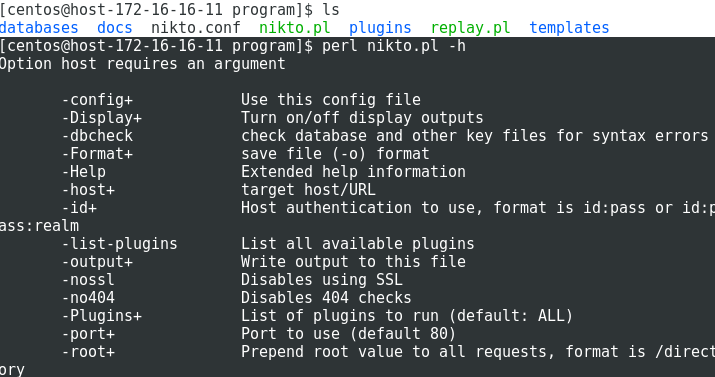
$ nmap -v -sS -A -T4 172.16.16.7



**Nikto**

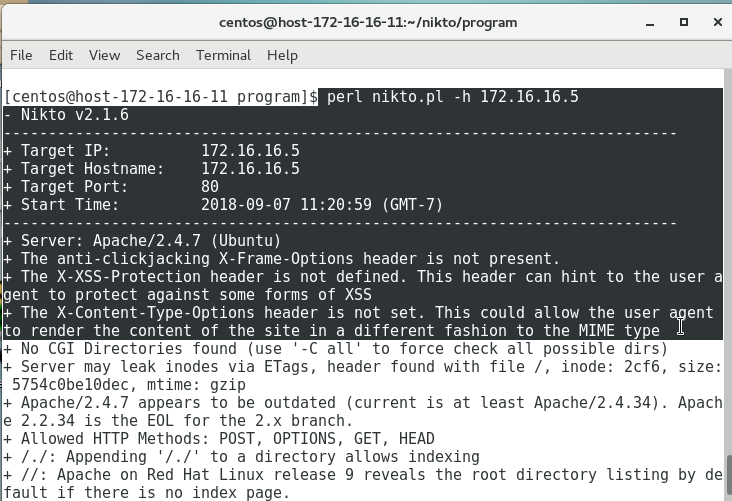
Web application and CGI scanner

1. $ sudo yum install git perl perl-Net-SSLeay openssl
2. $ sudo git clone <https://github.com/sullo/nikto.git>
3. $ cd nikto/program
4. $ perl nikto.pl -h



5. Basic testing using nikto

$ perl nikto.pl -h 172.16.16.5

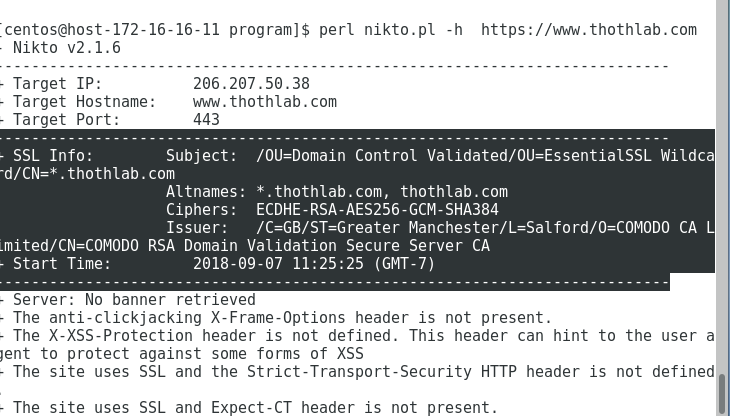


6. Testing specific port

$ perl nikto.pl -h 172.16.27.56 -p 443

7. Scanning a vulnerable website

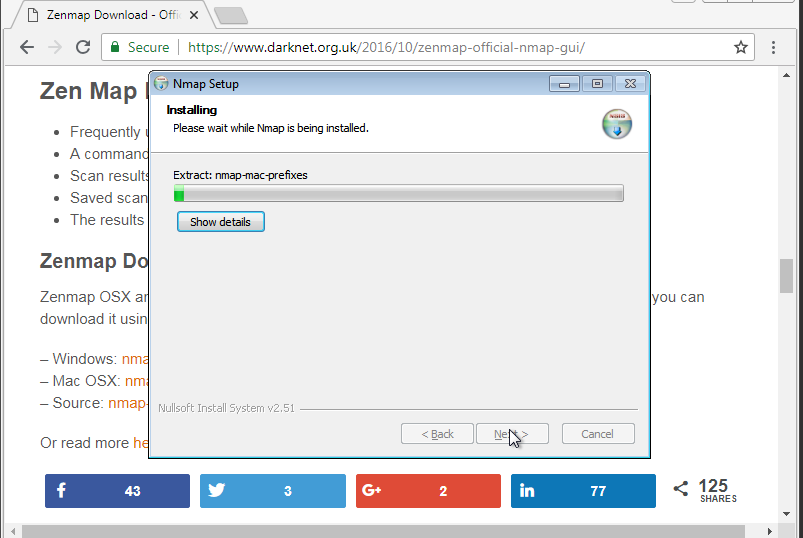
$ perl nikto.pl -h <http://www.thothlab.com>



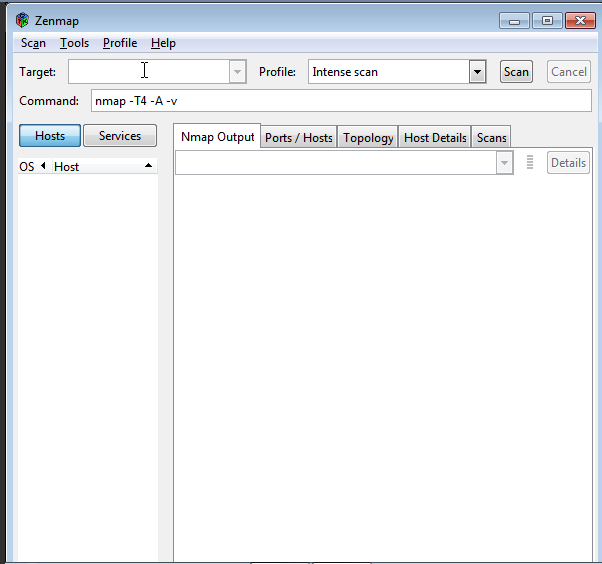
**Zenmap**

Windows alternative to nmap

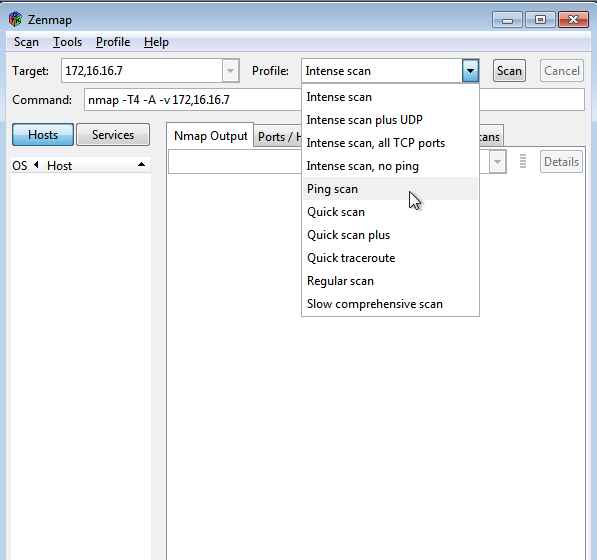
1. Download and install, set up will ask for installation of WinPCAP, so make sure you allow permission to install WinPCAP

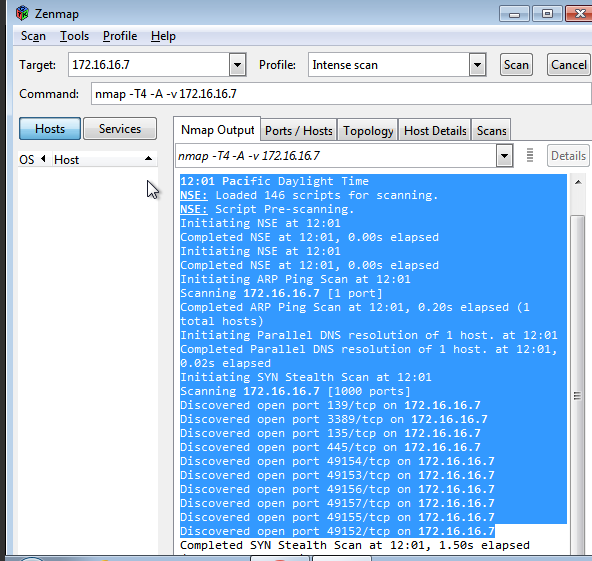


2. Start ZenMAP GUI

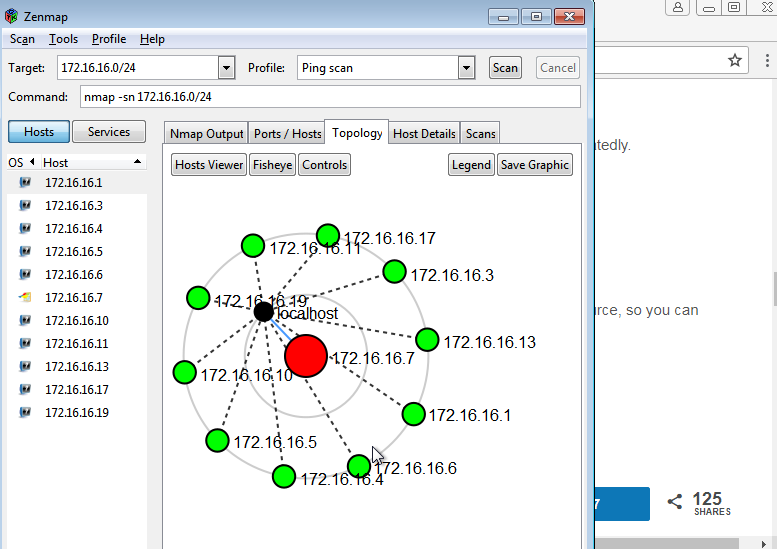


3. You can scan a single host or a range of hosts

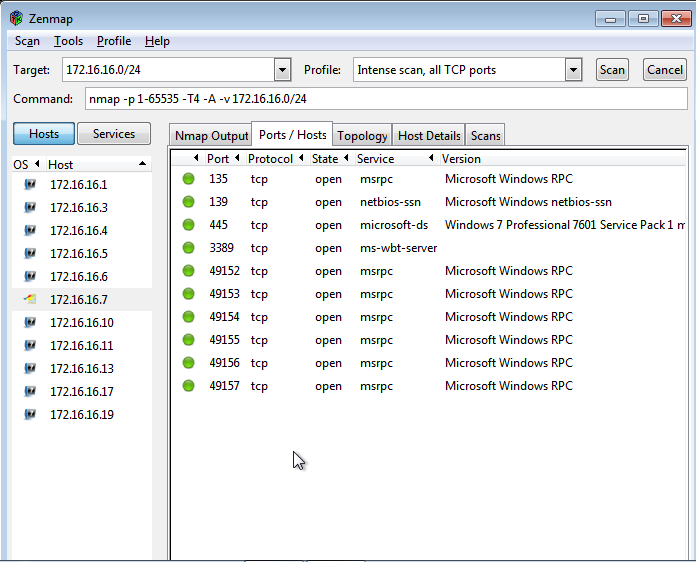


****

4. Ping scan and topology visualization



5. Scanning TCP ports using Zenmap

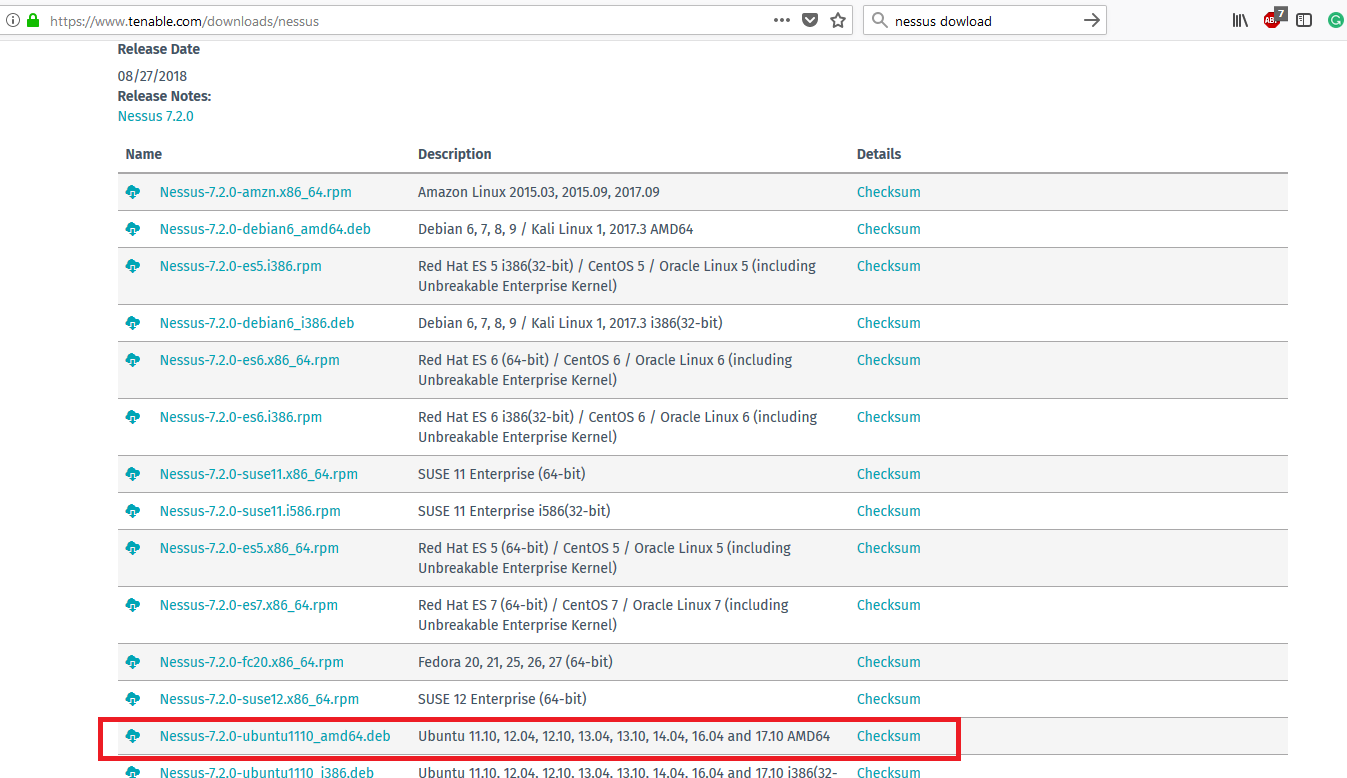


**Nessus**

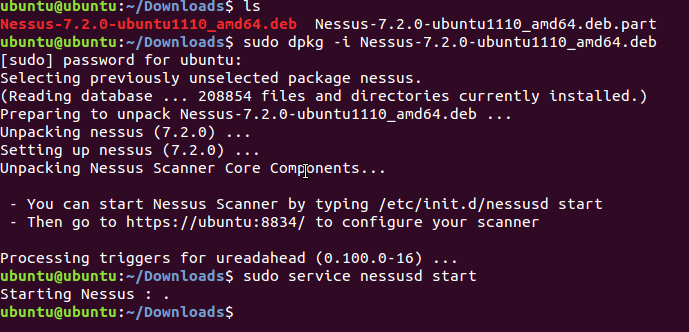
Vulnerability Scanner

1. Download Nessus from tenable website

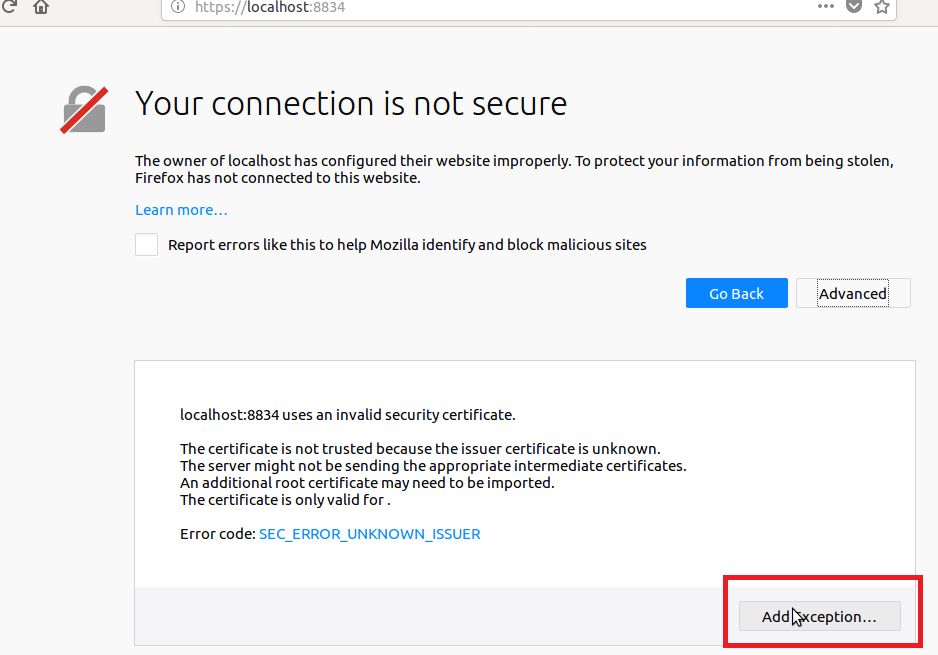
https://www.tenable.com/downloads/nessus



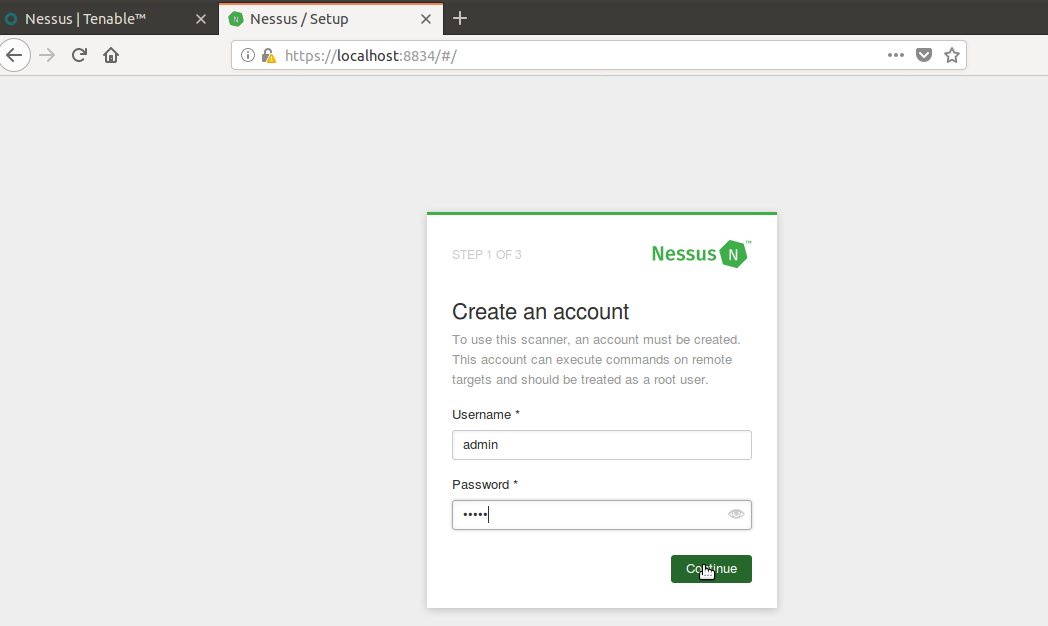
2. Install the downloaded nessus package and start the Nessus Service



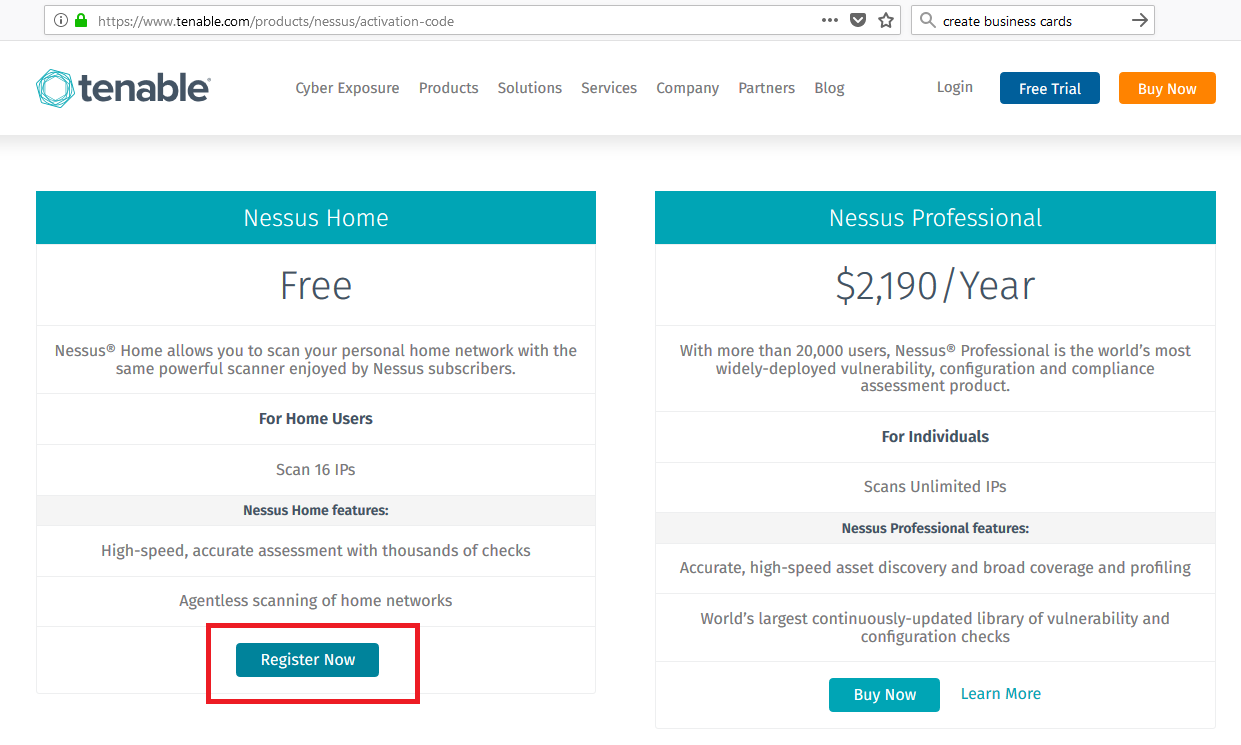
3. Browse the URL, [https://localhost:8834](http://localhost:8834)



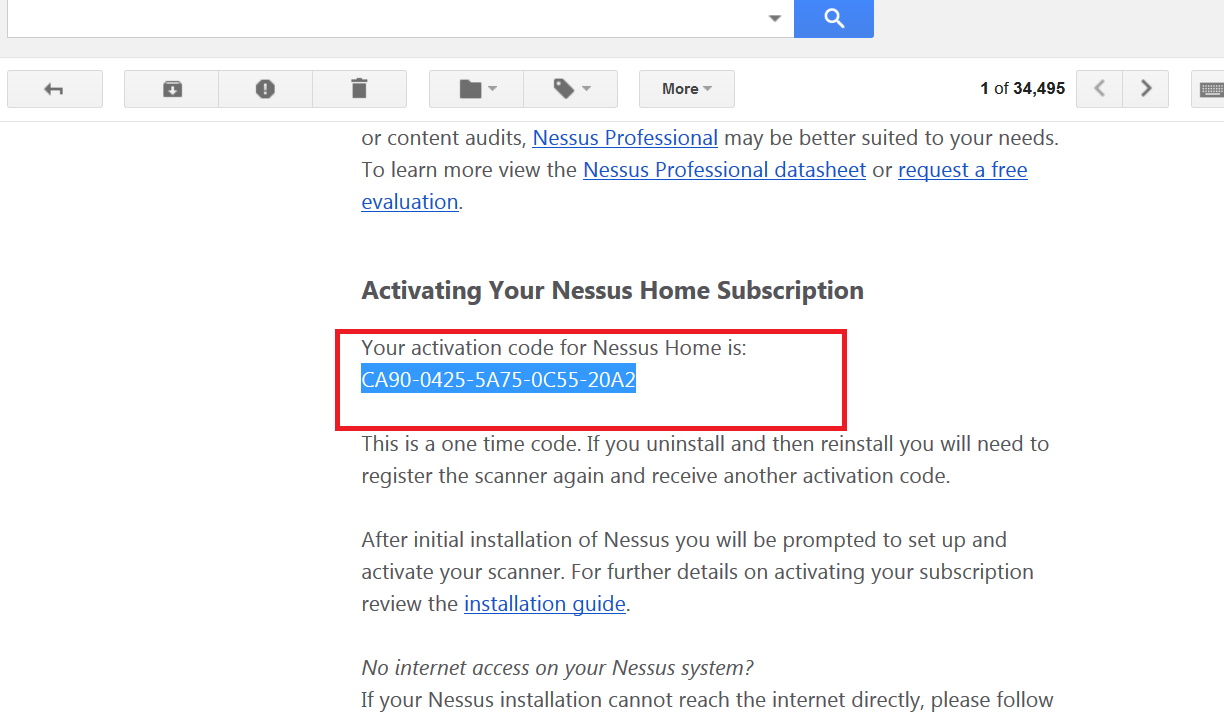
4. Create an account “admin/admin”

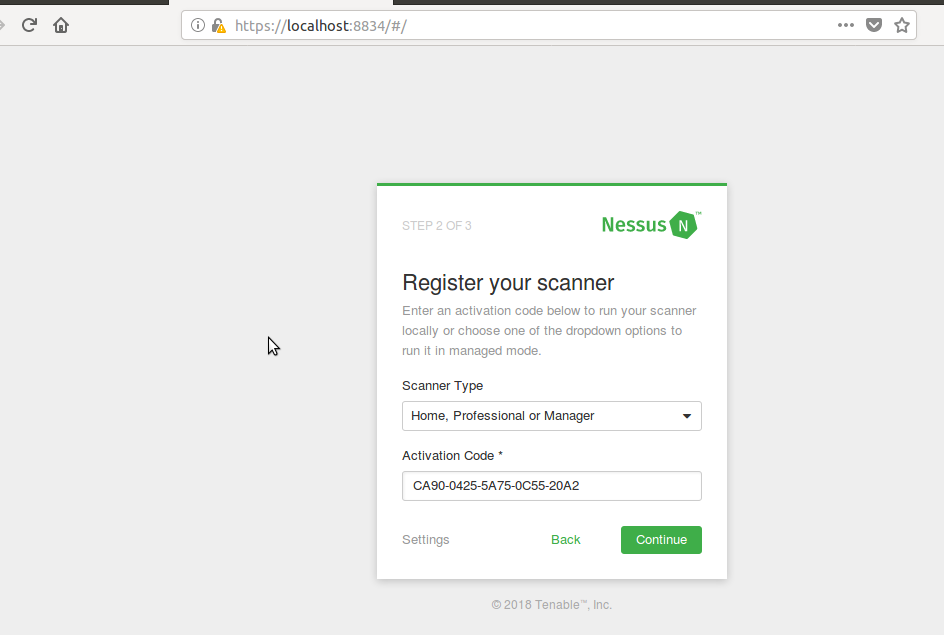
****

5. <https://www.tenable.com/downloads/nessus> - Get activation code

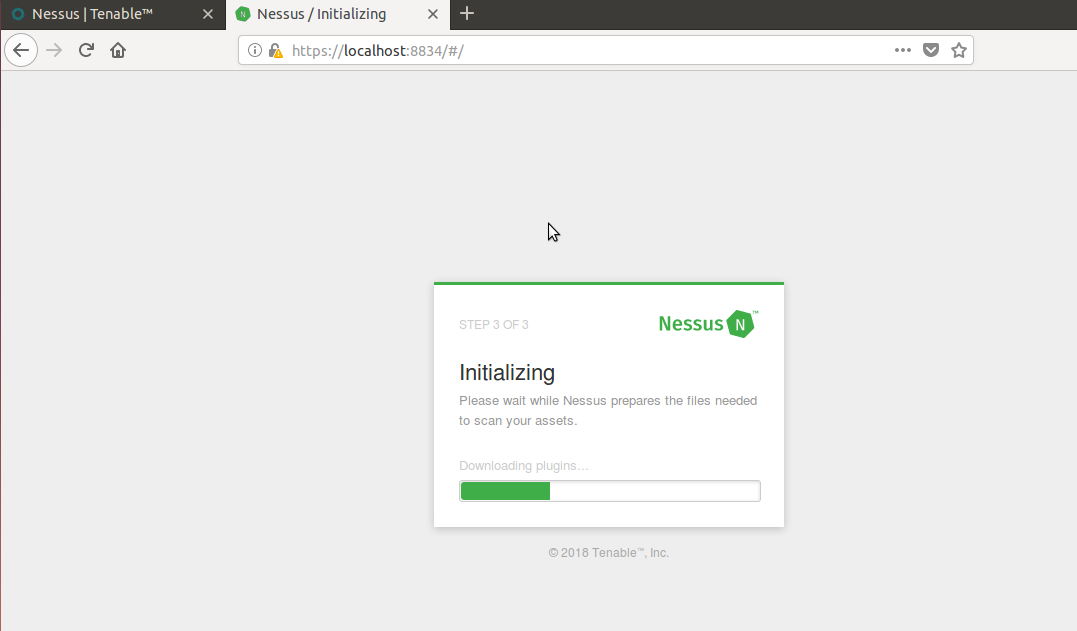


6. Enter the activation code received in email

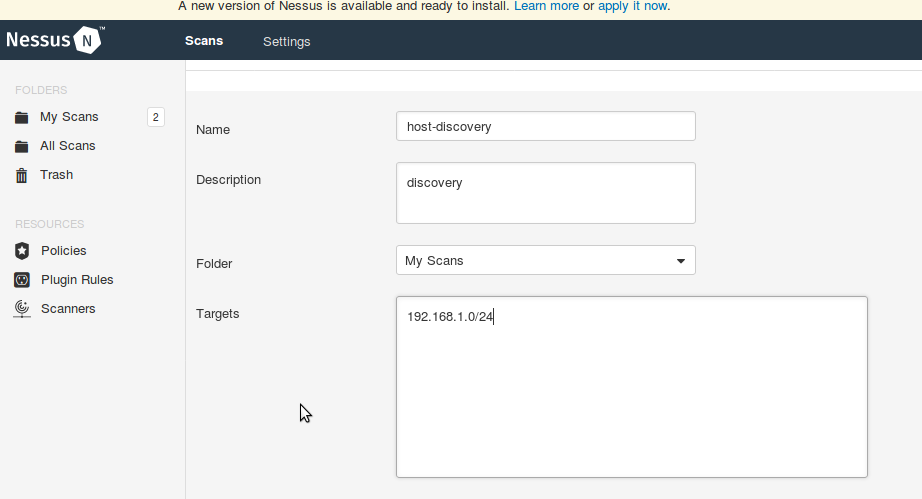
****

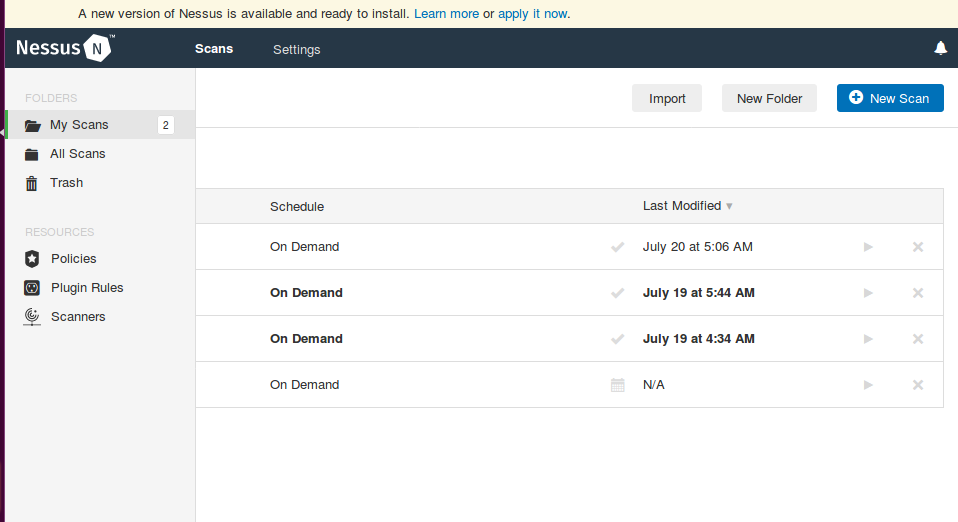


7. Initialization can take some time

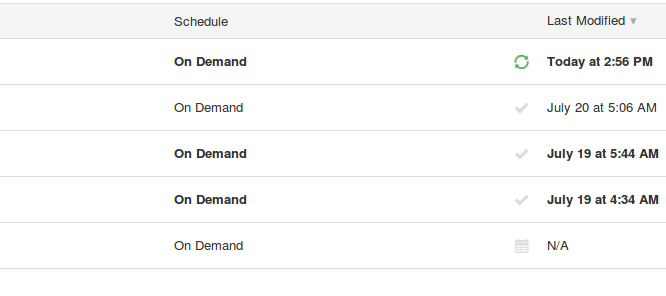
****

8. Create new scan

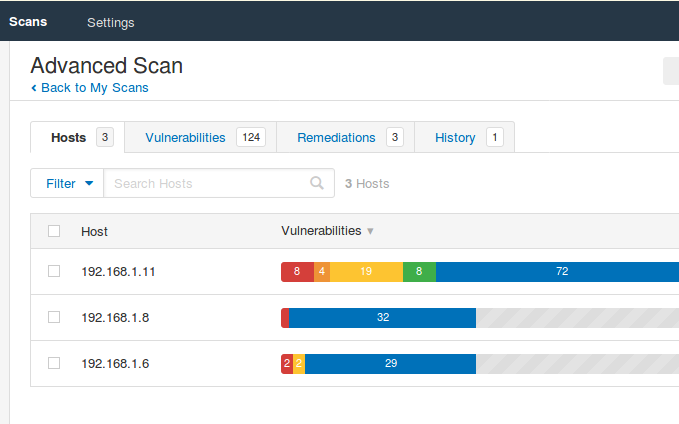
****

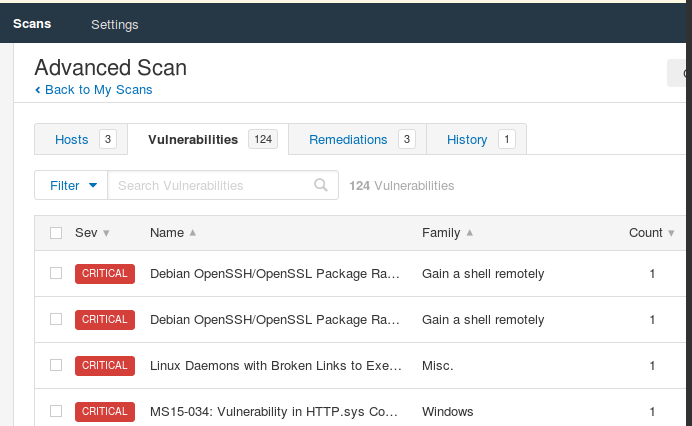
****

9. Launch the scan

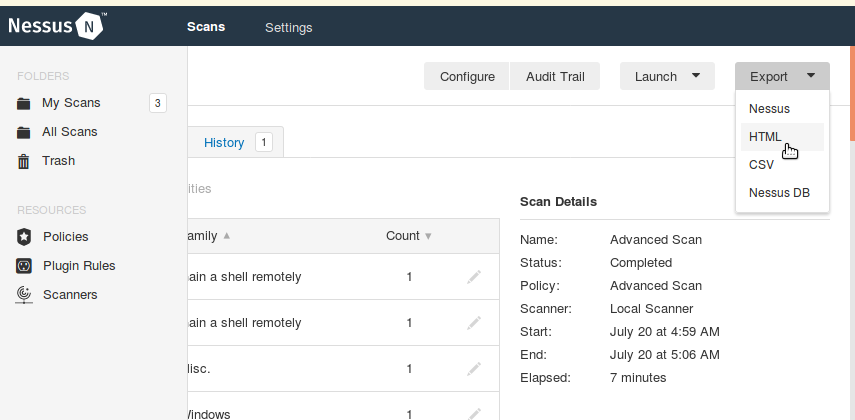
****

10. Check Scan Results and vulnerabilities

****

****

11. Export Scan Data

****

**References**

<https://nmap.org/book/man-briefoptions.html>

https://highon.coffee/blog/nmap-cheat-sheet/