**Workflow for Automated Web Application and Host Vulnerability Assessment**

Table of Contents

[I. Overview 2](#_Toc405879434)

[II. Tools 2](#_Toc405879435)

[III. Web Application Security Assessment 2](#_Toc405879436)

[1. Target Verification 2](#_Toc405879437)

[2. Identifying Hosts with Web Application Using Nmap 2](#_Toc405879438)

[3. Scanning for Application Vulnerabilities Using BurpSuite Pro 3](#_Toc405879439)

[3.1. Adding Nmap-scanned Hosts to Burp Suite as Targets 3](#_Toc405879440)

[3.1.1. Opening Nmap scan result 3](#_Toc405879441)

[3.1.2. Initial connection to the target site using Burp Repeater 4](#_Toc405879442)

[3.1.3. Adding Application URL to Burp’s Site map 5](#_Toc405879443)

[3.1.4. No Response on port 80, Try 443 6](#_Toc405879444)

[3.1.5. No Response, Try Changing User-Agent 7](#_Toc405879445)

[3.1.6. Adding Application URL into Burp Suite’s Global Scope 9](#_Toc405879446)

[3.2. Spidering the Web Application using Burp Spider 9](#_Toc405879447)

[3.2.1. Spidering while interacting with web application (passive spidering) 10](#_Toc405879448)

[3.2.2. Spidering by manually launching Burp Spider (active spidering) 11](#_Toc405879449)

[3.2.3. Combining Active and Passive Spidering 12](#_Toc405879450)

[3.2.4. Discovering Hidden URLs through Content Discovery 14](#_Toc405879451)

[3.3. Scanning Web Application for Vulnerabilities using Burp Scanner 16](#_Toc405879452)

[3.3.1. Scanning actively by manually launching Burp Scanner 16](#_Toc405879453)

[3.3.1.1. Viewing the Status of On-going Scans 18](#_Toc405879454)

[3.3.2. Scanning actively while browsing the web application 19](#_Toc405879455)

[3.3.3. Creating report for discovered vulnerabilities 19](#_Toc405879456)

[4. Scanning for Web Application Vulnerabilities Using Nmap Scripts 20](#_Toc405879457)

[5. Scanning for Application Vulnerabilities Using Qualys Web Application Scanning 20](#_Toc405879458)

[IV. Host/Network Services Vulnerability Assessment 20](#_Toc405879459)

[1. Identifying Live Hosts with Open TCP and UDP Ports Using Nmap 20](#_Toc405879460)

# Overview

# Tools

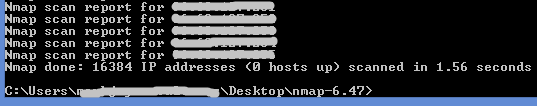
* 1. Nmap
  2. Burpsuite Pro
  3. Qualys/Nexpose, etc.

# Web Application Security Assessment

## Target Verification

Nmap supports target hosts in various notations such as CIDR as well as octet ranges (e.g.,x.x.x.x***/18*** or x.***x-x***.x.***x-x***). To see how many IPs we are looking at:

*nmap x.x.x.x/18 -sL –n*

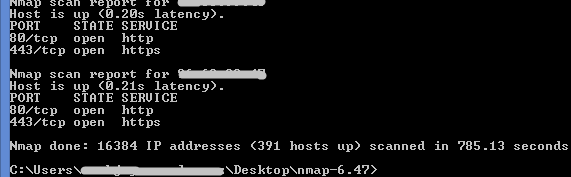
**

## Identifying Hosts with Web Application Using Nmap

For web application testing, we are only interested in hosts with reachable 80,443 (those that respond to SYN-ping (*-PS80,443*) on those two ports. If they are live and not firewalled, then we scan if those ports (*-p80,443*) are actually open. Nmap uses SYN scan by default and falls back to TCP Connect for unprevileged users, so we need not specify any port scan technique here.

We save the scan result into a *grep*-able format (*-oG x.x.x.x.gnmap*) and xml (*-oX x.x.x.x.xml*) that can be opened in Excel. We only include in the report the live hosts having any of those http/s ports open (*--open*) to avoid cluttering our output. We limit our service probe retries to 1 (*--max-retries*) and and run the scan in aggressively probe (*-T4*) to speed things up. We just want to know if those web ports are open or not so we don’t do any further service version and OS detection.

*nmap x.x.x.x/18 -PS80,443 -p80,443 -oG x.x.x.x.gnmap –oX x.x.x.0.xml --open --max-retries 1 -T4*

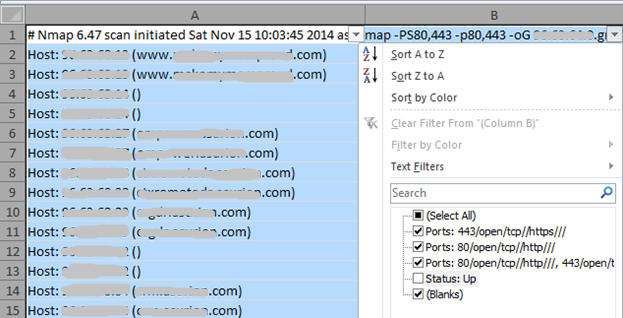
**

## Scanning for Application Vulnerabilities Using BurpSuite Pro

### Adding Nmap-scanned Hosts to Burp Suite as Targets

### Opening Nmap scan result

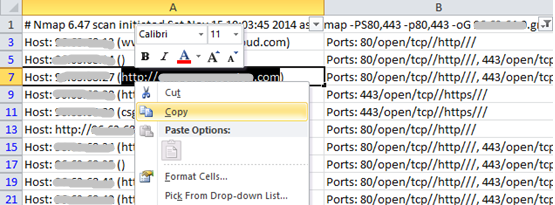
Open grep-able nmap scan output (#2) in Excel (tab-delimited). Filter out lines containing host status to tidy up the list and remove duplicates.

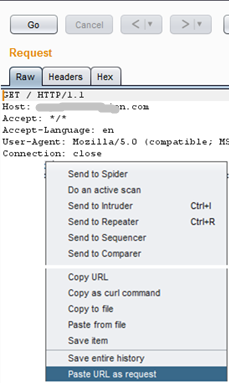


### Initial connection to the target site using Burp Repeater

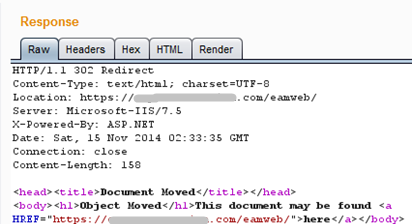
This is the first step before any website can be added to Burp for scanning. It will enable Burp to retrieve a page, in this case, the root(/) of the target web application as a starting point for any subsequent spidering.

Paste each hostname/URL (if nmap was able to resolve, otherwise just use the IP address) into Repeater as a request (must prepend with http:// or https://), depending on which port (either 80 or 443 or both) was detected by nmap to be open.



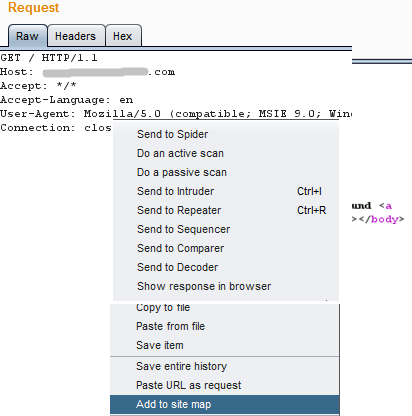


Send the request and wait for a response.



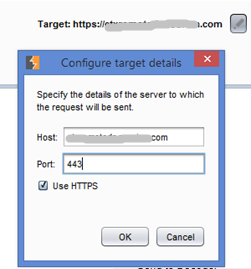
### Adding Application URL to Burp’s Site map

Once response is received, add the URL into Sitemap. Do both steps (3.1.2, 3.1.3) for each website to be tested. Burp’s Site map is a place where all the URLs to be tested will be listed (Target->Site map tab).



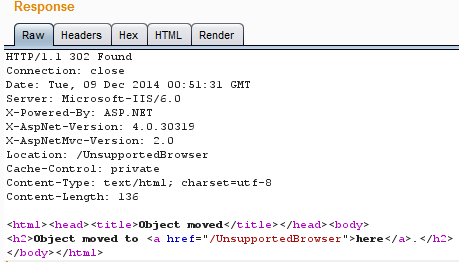
### No Response on port 80, Try 443

If no response is received (e.g. on port 80), the site may only be accessible using HTTPS. Target details can be modified in Burp Repeater (upper right corner). It is important to get a response, otherwise, this host/URL cannot be added to Site map, and thus cannot be actively scanned using Burp Scanner or tested with any other Burp tool.



### No Response, Try Changing User-Agent

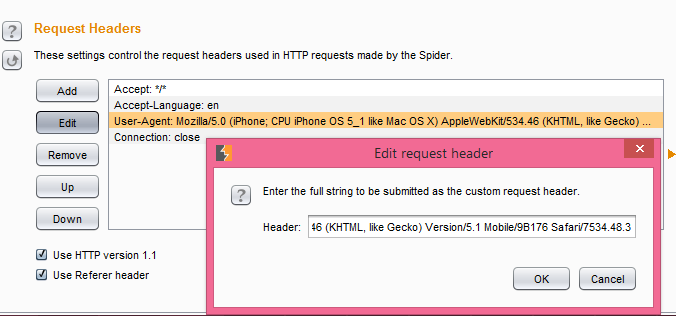
Sometimes, some sites such as mobile applications only respond to web requests if the requesting client is a mobile device.



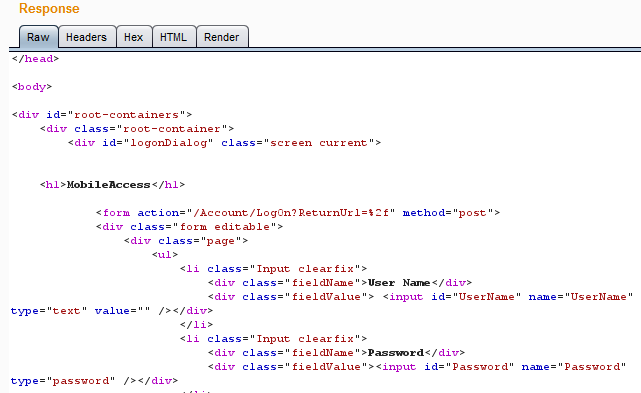
To get the initial response the User-Agent used by Burp Repeater must be changed to a mobile device User-Agent such as:

*User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5\_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3*

This can be set by accessing the Options tab of Burp Spider:



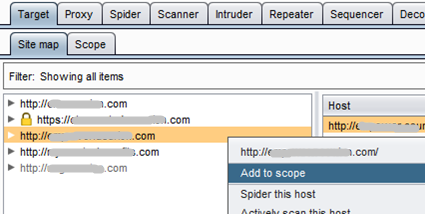
Once the User-Agent has been changed, a ddiferent response is received, this time indicating that the browser is now supported.



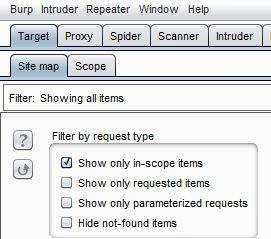
### Adding Application URL into Burp Suite’s Global Scope

URLs can be scanned later without being added into Burp’s global scope. However, to ensure that we don’t accidentally spider or scan sites that are out-of-scope, the target URLs must be added into Burp Suite’s global scope. Additionally, when these out-of-scope URLs appear in the Site map while spidering, they can be hidden by enabling filtering by request type.

To add the target sites into scope, go to Target->Site map, then add each URL into scope.



After adding all the hosts into scope, enable filter by request type (Show only in-scope items).



### Spidering the Web Application using Burp Spider

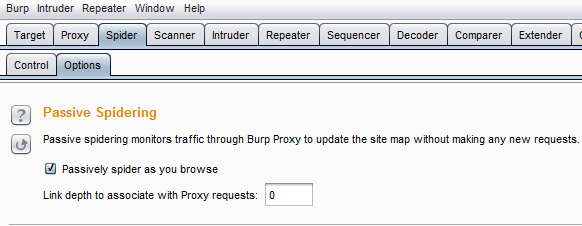
This is one of the most critical steps that must be done prior to scanning for vulnerabilities because without identifying all URLs or web application pages that can accept parameter value submissions, Burp Scanner will not be able to identify any injection vulnerability (e.g., XSS, SQL injection, OS command injection, etc.)

Two steps are essential when Spidering the web site; passive spidering and active spidering.

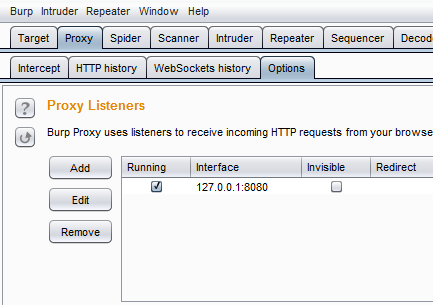
### Spidering while interacting with web application (passive spidering)

Burp Spider can reveal resources or URLs in a web application while browsing that application (w/ the help of Burp Proxy).

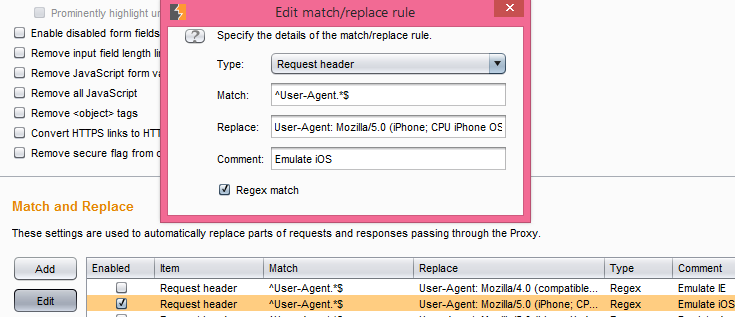
To enable Passive Spidering, set Burp Spider to “Passively spider as you browse” as shown below:



Then enable Burp Proxy listener and set your browser to use it. Finally browse the application being tested.

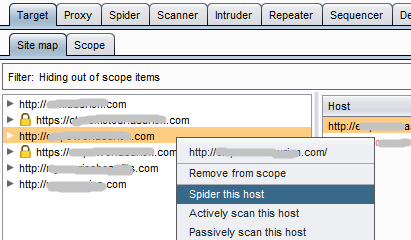


Additionally, if dealing with a web application that only accept requests from mobile devices, Burp Proxy’s User-Agent can also be changed in the Options tab:



### Spidering by manually launching Burp Spider (active spidering)

To Spider each in-scope URL in the Site map manually, right click on the URL then select “spider this host”. Burp Spider will extract and follow every link it can find in every web page starting from the site’s root (/) as well as those in robots.txt if it finds one.

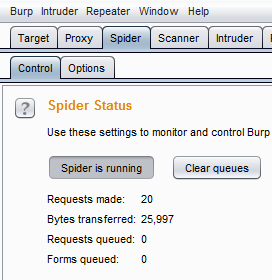
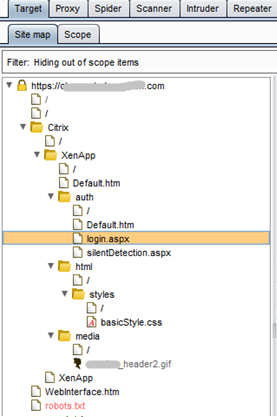


### Combining Active and Passive Spidering

Spidering by browsing the application (passive) is important because when spidering by launching Burp Spider manually (active), it is unable to parse or execute certain tags in the server response such as java scripts. If a java script is suppose to load an additional page, Burp Spider could miss that page and all the links embedded in it.

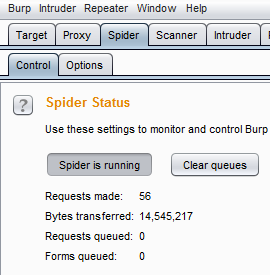
*Ex.* [*https://www.mysite.com*](https://www.mysite.com)

**Active Spidering:**



**Passive Spidering:**

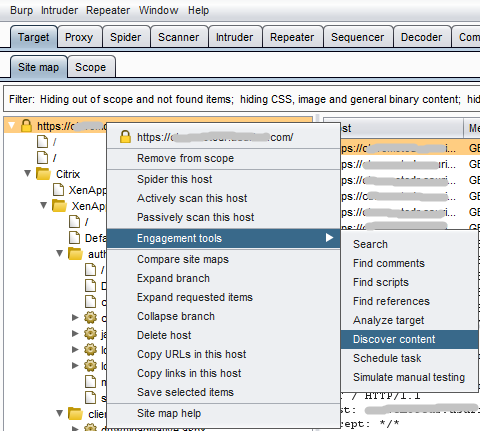
Additional pages with parameters are revealed when passive is combined with active spidering. These additional pages can then be tested with Burp Scanner using various injection techniques.

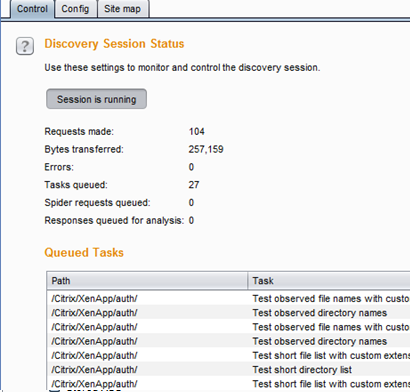
****

### Discovering Hidden URLs through Content Discovery

<loop error placeholder>

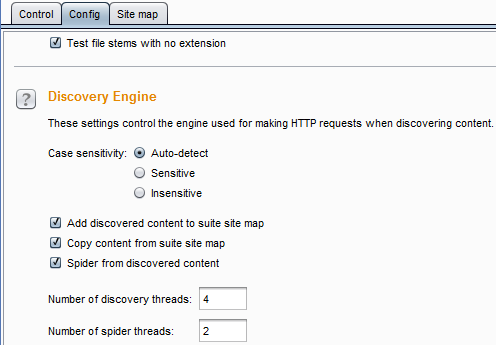
Aside from spidering, additional hidden contents or URLs can also be revealed by using Burp’s Content Discovery feature. Burp uses a variety of guessing or fuzzing techniques to accomplish this. Content Discovery can be accessed through the context menu as shown below.





The Site map tab above will contain the original Site map populated earlier, plus the newly discovered hidden URLs.

To ensure that those new items get added automatically to Burp’s original or global suite Site map, enable “Add discovered content to suite site map” from the Config tab. This is the default behavior.



### Scanning Web Application for Vulnerabilities using Burp Scanner

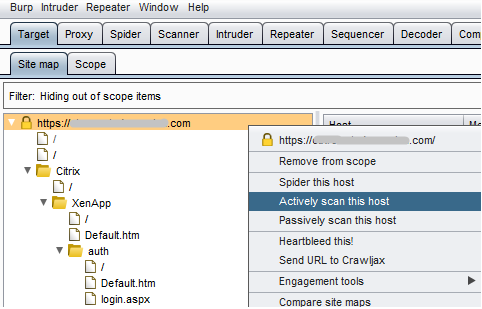
Just like when spidering, target web applications can also be scanned in two ways, by selecting them in the Site map and launching Burp Scanner from the context menu, or while interacting with the web application after setting your browser to use Burp Proxy (see section 3.2.1 to see how to set up Burp Proxy).

The type of scan to be performed can be active (Burp Scanner will inject different values to URLs or forms containing parameters), or passive (Burp Scanner will only analyze existing traffic e.g., after the site has been spidered and will not send any new requests). The former yields better result since Burp Scanner can inject different values to the application.

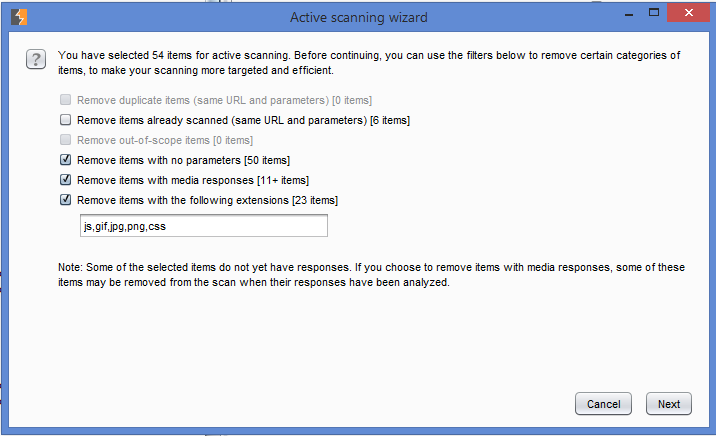
### Scanning actively by manually launching Burp Scanner

One can actively scan the target site by accessing the right-click context menu and selecting “Actively scan this host”.

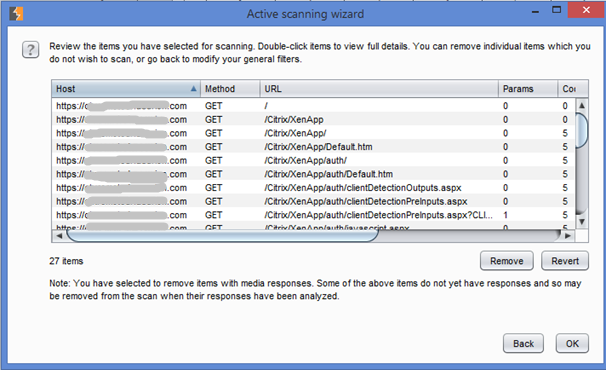
Individual URLs can also be tested selectively (right-click context menu -> “Do an active scan”). This is useful if you want to test only the URLs containing parameters and skip those that don’t.



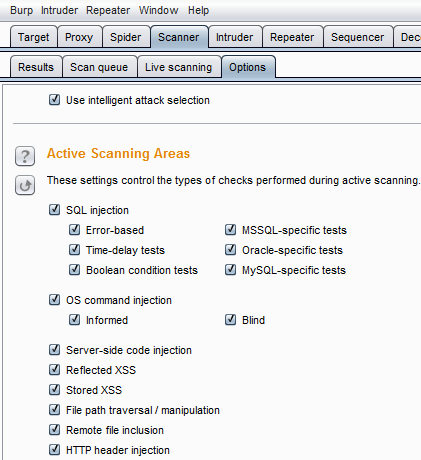
Launching Burp Scanner from the context menu will launch the Active scanning wizard where items that you do not want to be included in the scan (such as those URLs that do not have parameters) can be specified. Items that have already been scanned can also be skipped.



A final confirmation window containing a list of items or URLs that will be scanned is presented where additional items that you want to exclude can be removed.

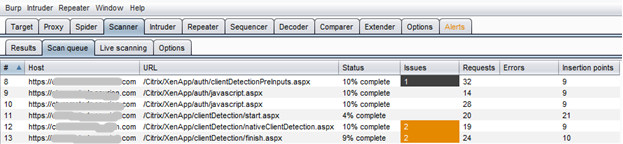


Areas to be tested as well as the insertion points (where test values can be injected) can be set in the Burp Scanner’s Options tab.



### Viewing the Status of On-going Scans

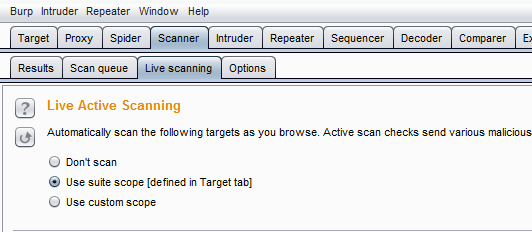
Status of any on-going scan can be viewed by accessing Scanner->Scan Queue as shown below. Any scan can also be cancelled by selecting the URL and accessing the right-click context menu.



### Scanning actively while browsing the web application

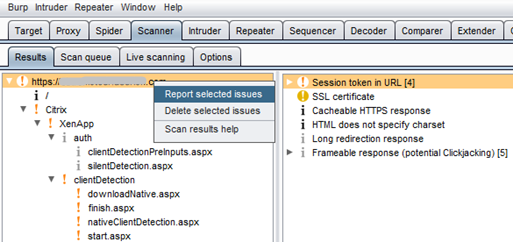
Burp can also scan for vulnerabilities while you are interacting with the application using a browser. This is useful if you want to select areas in the web application that you want to test while seeing them in your browser.

This process is called Live Scanning. To enable Live Active Scanning, set Burp Scanner to “Automatically scan targets as you browse”.



### Creating report for discovered vulnerabilities

When Burp Scanner has finished scanning all selected targets (see Scanner->Scan queue), a consolidated report (Scanner->Results) can be exported into an HTML or XML format:



## Scanning for Web Application Vulnerabilities Using Nmap Scripts

## Scanning for Application Vulnerabilities Using Qualys Web Application Scanning

# Host/Network Services Vulnerability Assessment

## Identifying Live Hosts with Open TCP and UDP Ports Using Nmap

For general network service vulnerability assessment, the first step is to conduct a network discovery to identify hosts that have remotely-accessible network services listening on open TCP and UDP ports. This procedure is similar to discovering hosts running web application previously discussed (Sec. III-2).

Finding out which hosts that are alive can be accomplished easily, however, finding out which TCP and UDP ports are open on every host can be challenging in terms of duration depending on how accurate you want to do your scan and how many IPs you are dealing with. There are 65535 possible TCP and as much UDP ports that those live hosts may be serving and your scan can last from just a few minutes, upto several days.