What did you do?:

The purpose of this week’s exercise is to check for network vulnerabilities using ShieldsUP! and Nessus on our home network. After doing some preliminary research on how both products function, first up was ShieldsUP!. ShieldsUP! is a port scanning tool that can help identify any potential vulnerable ports in a network. It is important to note that similar to most network security software, port scanners can be used for malicious purposes as well. These programs can allow hackers to find vulnerabilities in your network that can allow them to hack your network. ShieldsUP! works by sending packet connection requests to the network to pre-specified ports (marked by the user) and then noting the responses or lack thereof. There are three different types of responses that can be given by ports and they are either Open, Closed, or Stealth. An Open port reading means that the port is accepting and creating a connection with the test packet being sent. A port with this reading is most vulnerable, as it is actively preparing to accept unsolicited connection request packets from anonymous and unknown machines, obviously opening the network to potential hacks. The second port type is Closed, and a Closed port indicates that while the port does not accept any package requests the scanning program can still see that port is there. Ports that return a closed status may not be directly in danger now as they refuse the connection, however it is still not the ideal and safest state as it is still identified as existing. This could potentially allow hackers to mark down the port information and periodically revisit to attempt a connection again. The last and most secure port status is Stealth. A Stealth status indicates that the port didn’t respond in any way to the packet request. Instead of rejecting or accepting the request like closed or open status, Stealth status simply ignores the request and thus the port scanner cannot even identify that it is there, making the port invisible. This is the most ideal status as it doesn’t allow for outside sources to connect to or even identify the port thus protecting the network from hacks. To execute the ShieldsUP! scans I headed to the Gibson Research Corporation’s website (grc.com) and found ShieldsUP! under the services tab. The task was to run two different scans, the first of which was the “Common Ports Scan” which scans the ‘most common and troublesome” ports. This scan took a total of 5 seconds and I had my results. ShieldsUP! made it relatively easy to do a quick visual check of the results, as it highlights any stealth ports in green, closed in blue, and open in red. ShieldsUP! also provided the service that uses the port so it was nice to be able to reference that mostly for the sake of increasing my understanding of the different types of services and how they may potentially use the ports. The color coding made it easier to focus on the results that were not in stealth, as the ports in stealth were secured and did not necessarily have to be researched any further. For the ports in non stealth statuses, ShieldsUP! also features the ability to learn more about the port and its service and explain why the port may be potentially open or closed. In addition to looking in the provided documentation I also tried googling the port number and the status, if it was not stealth, to see if there was any additional information I could find that would explain the status for the port. After feeling like I had a sufficient understanding of Common Port scan results, I moved on to running the “All Service Ports” scan, this scan checks the first 1056 ports. I was interested to see if results would vary from scan to scan, I assumed no, but was interested nonetheless. Once started, the scan took just under a minute and ten seconds. Similar to my approach with the common scan, ShieldsUP! again was color coded and made analysis easier as I was able to quickly identify the ports that were in stealth and those that were not. Again ShieldsUP! allowed me to learn more details about the un-stealthed ports however this time I came across a port that did not have any details outside of a service name, so I had to rely a little more on looking it up on the web to get more information.

The next portion of the test was to run a Nessus scan. Nessus is a vulnerability scanner that works by running plugins against hosts, these plugins identify which systems/services are running on which port, what components may be vulnerable to attacks and if compliance requirements are met. To go into a little further detail, after Nessus performs a host discovery, Nessus then runs a port scan, and then runs a service detection to determine which services are running in each port. After the ports/services are identified Nessus runs each host/service against a database of already known vulnerabilities to see if any are present. Nessus features a very user friendly interface that makes it easy to use and to understand and interpret results. Each potential vulnerability is given a color coded threat level, the levels are Critical, High, Medium, Low, and Info. In order to execute the Nessus scan, the first step was to download the program from Tenable. Since we are merely exploring the capabilities of the software, and the full version requires payment, the Nessus Essentials version was downloaded. This version allows for 16 IP addresses as opposed to the Professional version which does not have a limit. The Nessus Essentials version is free to use for students so I had to register with my school email and that provided a key that I used during the installation process to connect Nessus. This registration process also included creating a username and password for access. Nessus runs in an internet browser, and you are first prompted to log in. After login you are able to create scans and specify which IP addresses to scan. For my scan I identified my main computer's main IP address and then the IP address of my router (which was what was scanned by ShieldsUP!). The scan took a total of 6 minutes. After the scan was complete, I reviewed the details of each piece found in the scan within Nessus as it was pretty clear to understand what each piece found meant. There was also some documentation included that helped me interpret the results.

What were the results?:

The ShieldsUP! common port scan, scanned a total of 26 ports. Out of those 26 ports scanned all but 2 were in stealth status. The first non stealth port found was port 80, the HTTP port, and this port was in open status. Port 80 is the default port used to send and receive unencrypted web pages. It was quite startling to see an open port at first however after doing some research this could be the result of having to host a sql server site for my other summer course. Which would make sense as when hosting a site to the internet would require at least one port to be open and openly communicating. There is also a small possibility it also could stem from my network provider's configuration; it appears that this could be normal based on the fact that my ISP provided router uses a NAT(Network Address Translation) approach. This approach allows multiple private devices to connect to outside servers using the same shared external IP address. The NAT takes the private device's outgoing IP packets and then translates it to a different shared IP address that is used to connect with public networks. This applies the same way for incoming connections as well. External public networks will make connections with our

NAT shared public facing address and then the NAT will translate the destination to the proper private IP address. This creates an additional level of security by allowing devices IP addresses to stay hidden, due to the NAT translating all private IPs to the shared public one. The other port that did not turn back stealth was port 443 and this port came back as closed status. Port 443 is used for secured and encrypted web traffic. I was not quite as concerned with this as while the port is being identified communications are blocked the messaging is encrypted. For the “All Service Ports” scan a total of 1056 ports were scanned, as this is what the free version allows for. Prior to running this test I was wondering if there would be any major differences in terms of results between the All Service Port and Common Port scans. Obviously there are more ports scanned but I was curious to see if the results were going to be the same for ports 80 & 443, I assumed based on my understanding of how ShieldsUP! works that the results for these ports would be the same however I was still interested nonetheless. Out of the 1056 ports scanned all but 3 were in stealth status. Two of which were ports 80 & 443, and they both showed the same results. Port 80 returned as open and port 443 returned as closed. The additional non stealth port was port 554 and it returned open. This port is used for real time streaming protocol by either QuickTime streaming servers or by Windows Media streaming servers. From what I found in my research this can be a common setting with some routers however I do think it would be safest to investigate if there is a way I can get it stealth or at the very least close it. Overall the results of this scan are relatively positive however there is some slight cause for pause involving the open ports. My strategy to handle these issues is to wait until I turn off my class site, after the assignment is done graded, in my other class. I will then re-conduct the ShieldsUP! scans and see if there is any update on the non stealth ports. If not, I will then try to see if I can update any settings on the router. This may be tricky as the router is provided by my landlord, and I do not have administrative privileges. I am hopeful if this is the case that my landlord will be understanding and allow me to work with our ISP to make any necessary changes, if possible.

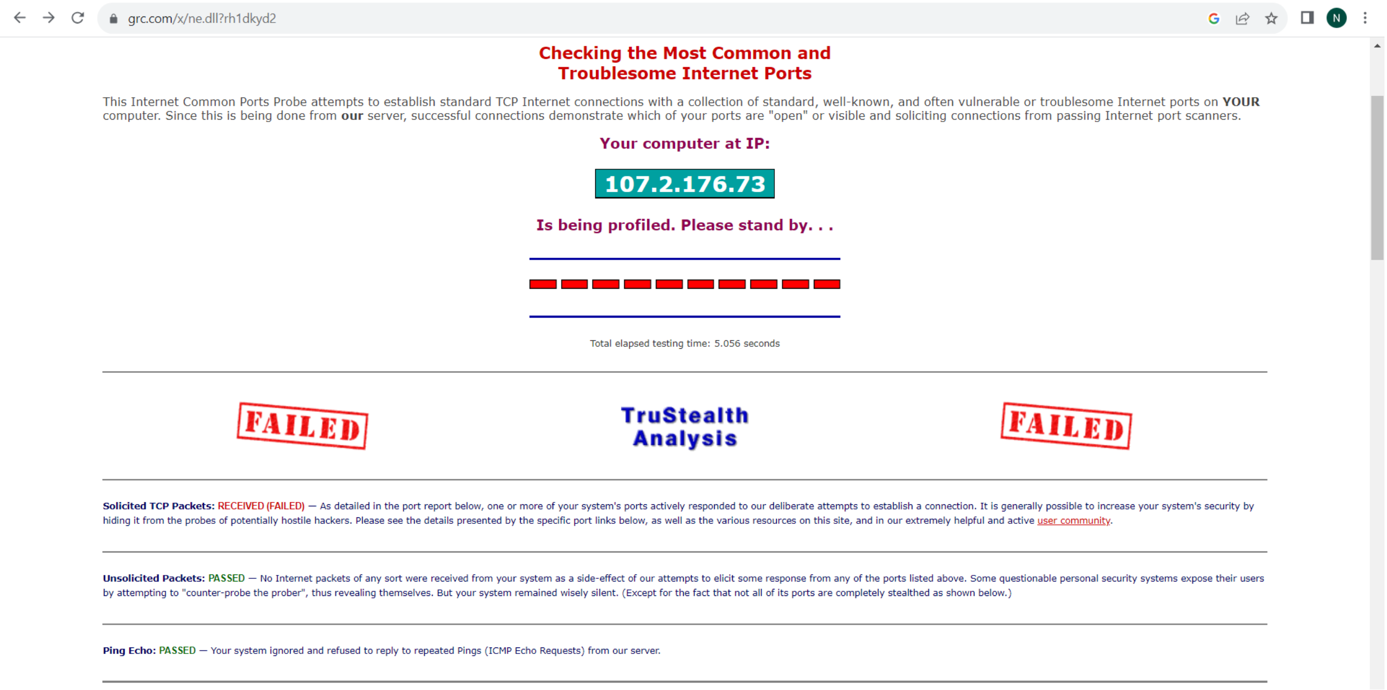
The results of the Nessus scan were from what I can tell very positive. The only type of vulnerability found in both scans fell under the Info category. From what I was able to find in the Nessus documentation and after some googling, the Info category does not indicate a vulnerability but is rather used to describe the action that is taking place. This was reassuring to see that there were no Vulnerabilities found. Obviously this does not mean that I am in a position to let my guard down. To get into further detail, my personal computer IP scan had a total of 3 Info vulnerabilities. The first was ‘Authenticated Check : OS Name and Installed Package Enumeration’ which is the plugin that logs into the host and extracts which packages are installed. The second was ‘Host Fully Qualified Domain Name (FQDN) Resolution’ which indicates Nessus was able to resolve the fully qualified domain name of the host. Which helps identify the machine. The third and final was, ‘OS Identification and Installed Software Enumeration over SSH v2’ which indicates Nessus was able to remotely log in to the host(my computer) using SSH or local commands and extract the list of packages that are installed.
For the router scan, a total of 14 info vulnerabilities were pulled back. The first was ‘Nessus SYN Scanner’ which is a port scanning plugin used by Nessus. The second was Service Detection’ which identifies which services are being used in the ports. Next was ‘Asset Attribute: Fully Qualified Domain Name (FQDN)’ which indicates that Nessus was able to identify the domain name. Then it was “Common Platform Enumeration” and this plugin reports the

hardware and software found on a host matches what is expected. After that it was ‘Device Type’ which is used to identified the type of device. This was pulled back as general-purpose which is interesting considering it is this IP address was a router. Next was ‘DNS Server Detection’ which provides a mapping between hostnames and IP addresses. Following was the ‘Embedded Web Server Detection’ that was followed by “Host Fully Qualified Domain Name (FQDN) Resolution”. Next was the “HTTP Server Type and Version” which is a plugin that attempts to determine the type and version of the remote web server. Following was ‘ICMP Timestamp Request Remote Date Disclosure’ which returns the time stamp on the host device. This can often be used by hackers to defeat time-based authentication protocols. The next was ‘Nessus Scan Information’ which provides the information about the Nessus scan including, Plugin Version, type of scanner, ports scanned, scan date and duration. Following that was the OS Identification, and TCP/IP Timestamps. The final info vulnerability was ‘Traceroute Information’ which shows the route used by the Nessus scan. As none of the results of the Nessus scan fell under the category of legitimate vulnerability I felt fairly confident and comfortable with the results. It is important to note that this ‘clean bill of health’ is only capturing a moment in time, and that it is important to frequently perform these checks and to have triggers in place to monitor any potential network changes. Additionally it may be good to use a different vulnerability scanner to see if results vary at all.

<u>What Did You Learn?:</u>

I think the most interesting thing to learn from this exercise was to see things from the perspective of hosting a site. I have run ShieldsUP! in the past however I was not hosting a site. My previous scan did not have any open ports and to be honest I expected the same this time around. This was obviously foolish in retrospect. This was an interesting angle to see, especially since I was only scanning my personal network where I generally only receive and not send. I would expect an organization's scan to be much more robust with all of the moving parts that can be involved. Additionally I think another big piece I learned, specific to my living situation, is that if you are given an already existing network as a part of your rental you cannot safely assume anything about your network security. You would hope that if a landlord was providing internet with the rental that they would at least due their due diligence in ensuring the connection is secure. However it is clear that the old adage of what can happen when you assume is in place here as well. I think it is safe to say that a majority of ‘normal’ individuals do not understand much about network security. It further supports the need that I was already fairly mindful of to be careful connecting to public networks, let’s be real. The individuals managing the network for a coffee shop may not have security on the brain.

Screenshots of Results:



Checking the Most Common and Troublesome Internet Ports

This Internet Common Ports Probe attempts to establish standard TCP Internet connections with a collection of standard, well-known, and often vulnerable or troublesome Internet ports on **YOUR** computer. Since this is being done from **our** server, successful connections demonstrate which of your ports are "open" or visible and soliciting connections from passing Internet port scanners.

Your computer at IP:

107.2.176.73

Is being profiled. Please stand by. . .

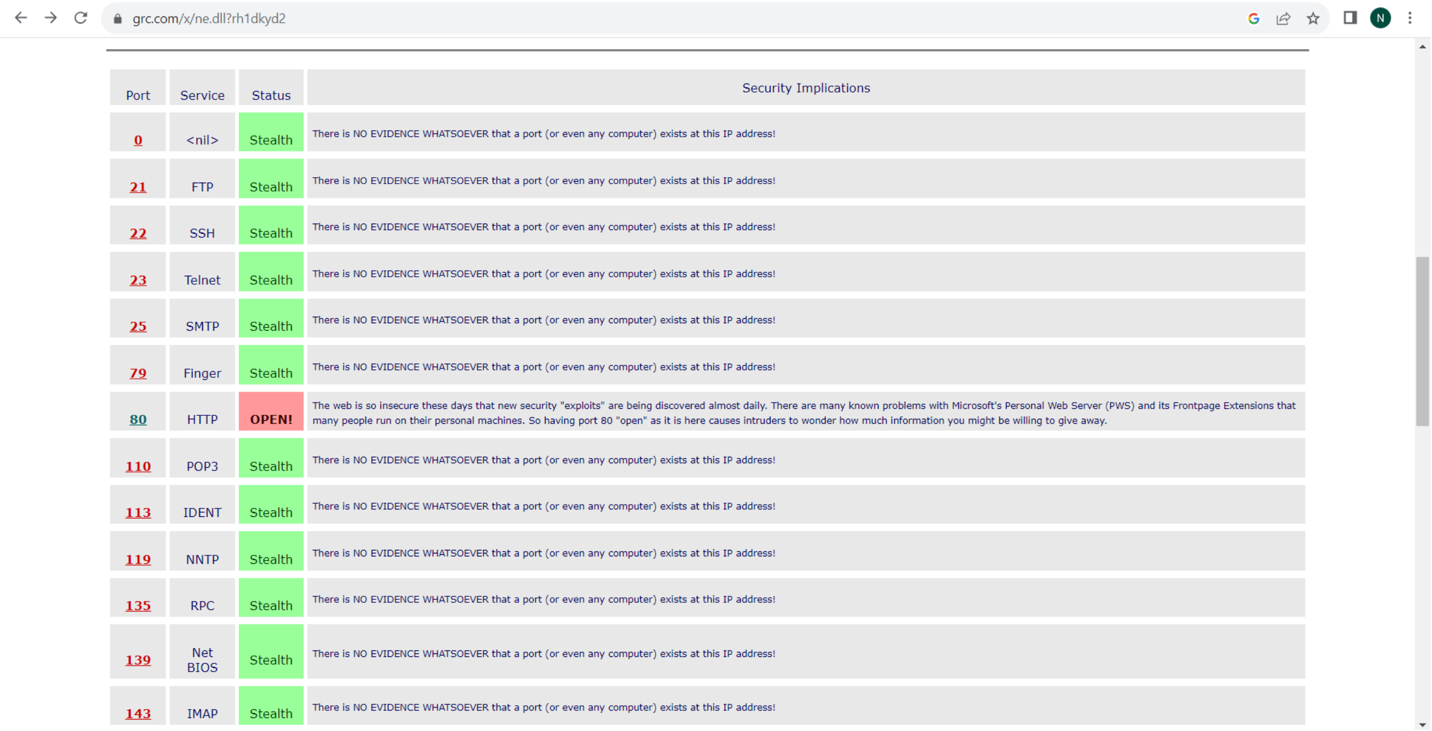
Total elapsed testing time: 5.056 seconds

FAILED **TruStealth Analysis** FAILED

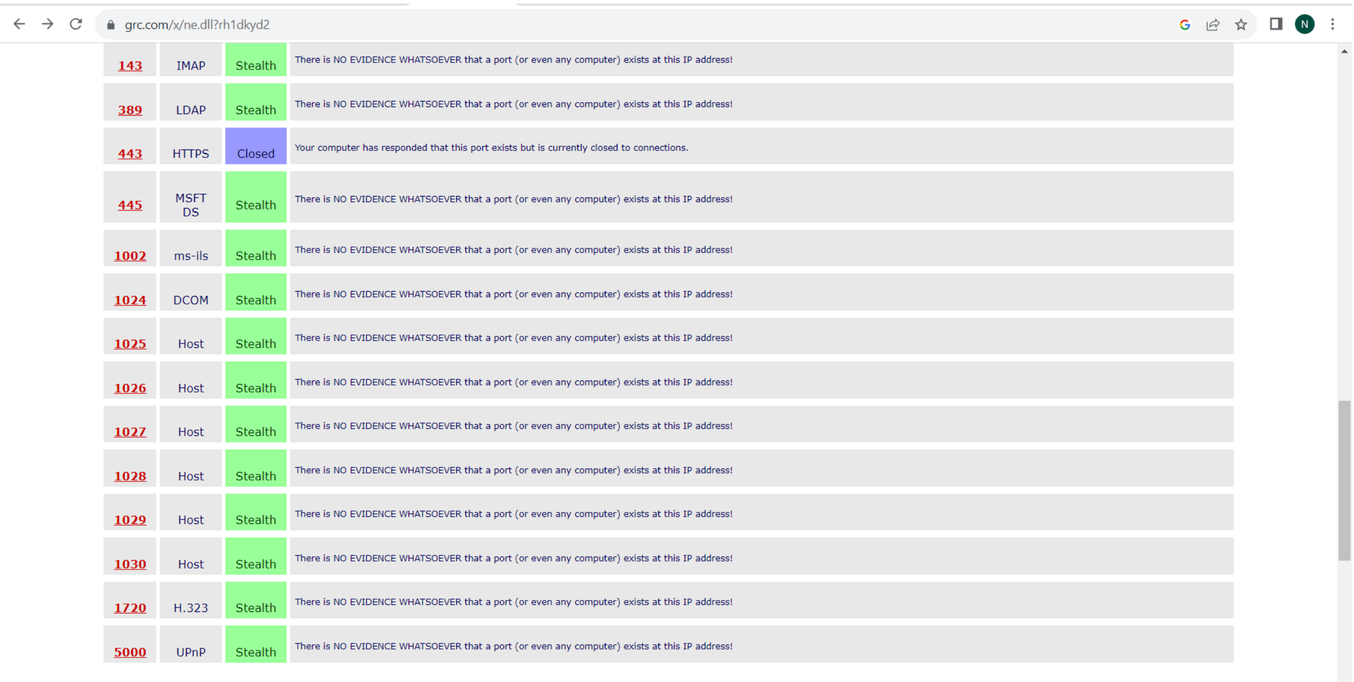
Solicited TCP Packets: RECEIVED (FAILED) — As detailed in the port report below, one or more of your system's ports actively responded to our deliberate attempts to establish a connection. It is generally possible to increase your system's security by hiding it from the probes of potentially hostile hackers. Please see the details presented by the specific port links below, as well as the various resources on this site, and in our extremely helpful and active user community.

Unsolicited Packets: PASSED — No Internet packets of any sort were received from your system as a side-effect of our attempts to elicit some response from any of the ports listed above. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system remained wisely silent. (Except for the fact that not all of its ports are completely stealthed as shown below.)

Ping Echo: PASSED — Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests) from our server.

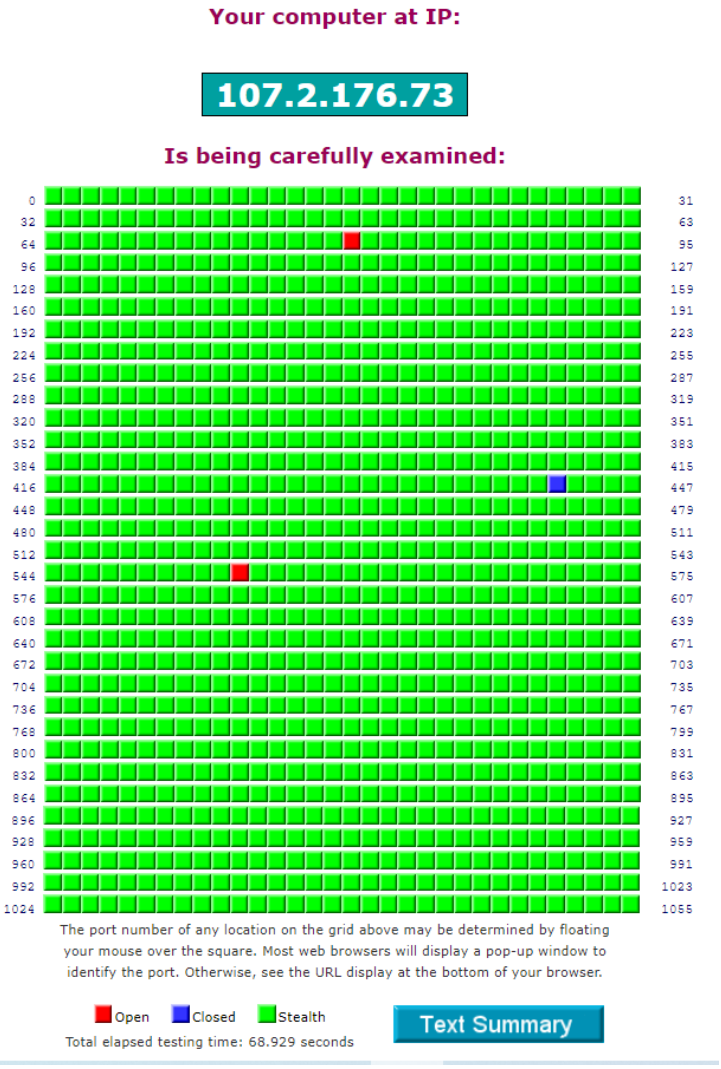


Port	Service	Status	Security Implications
0	<nil>	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
21	FTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
22	SSH	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
23	Telnet	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
25	SMTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
79	Finger	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
80	HTTP	OPEN!	The web is so insecure these days that new security "exploits" are being discovered almost daily. There are many known problems with Microsoft's Personal Web Server (PWS) and its Frontpage Extensions that many people run on their personal machines. So having port 80 "open" as it is here causes intruders to wonder how much information you might be willing to give away.
110	POP3	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
113	IDENT	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
119	NNTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
135	RPC	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
139	Net BIOS	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
143	IMAP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!



grc.com/x/ne.dll?rh1dkyd2

143	IMAP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
389	LDAP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
443	HTTPS	Closed	Your computer has responded that this port exists but is currently closed to connections.
445	MSFT DS	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
1002	ms-ils	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
1024	DCOM	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
1025	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
1026	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
1027	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
1028	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
1029	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
1030	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
1720	H.323	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
5000	UPnP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!



Your computer at IP:

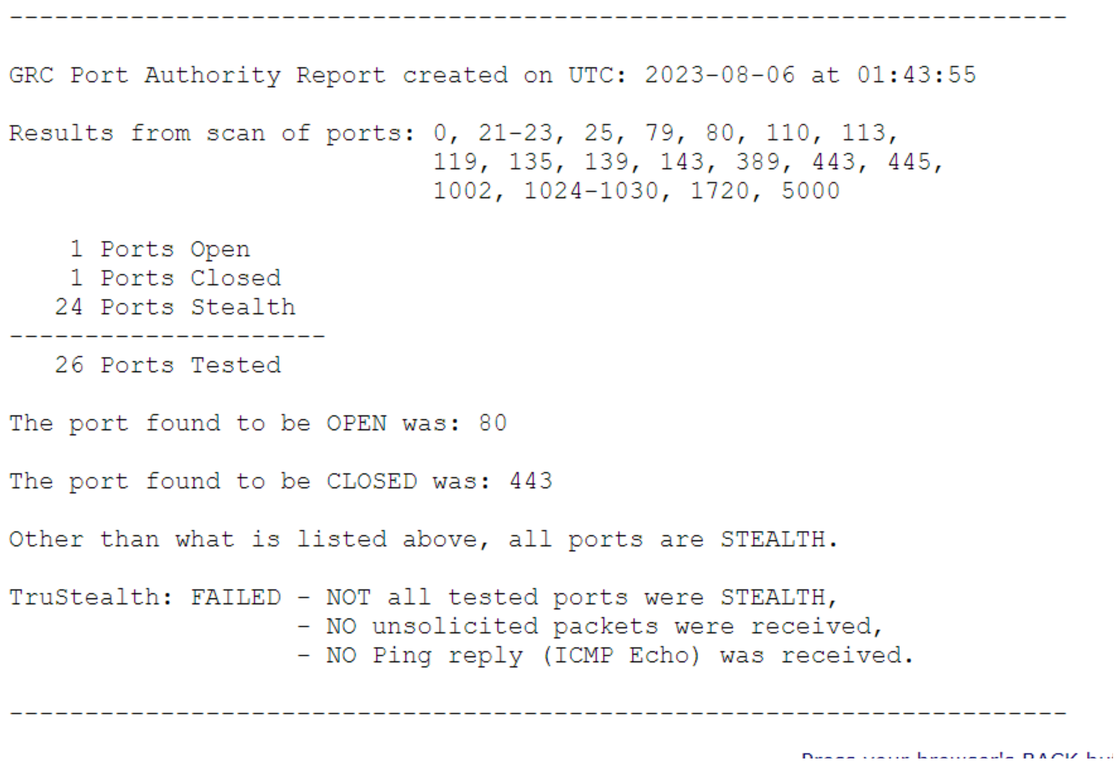
107.2.176.73

Is being carefully examined:

The port number of any location on the grid above may be determined by floating your mouse over the square. Most web browsers will display a pop-up window to identify the port. Otherwise, see the URL display at the bottom of your browser.

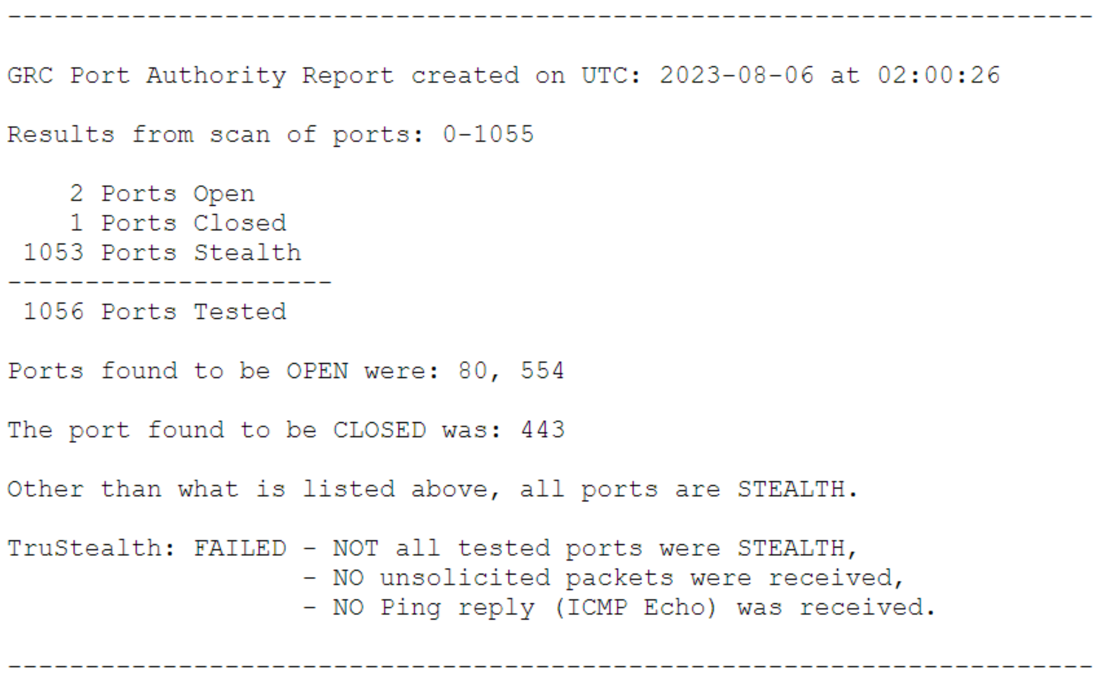
🟥 Open 🟦 Closed 🟩 Stealth

Total elapsed testing time: 68.929 seconds

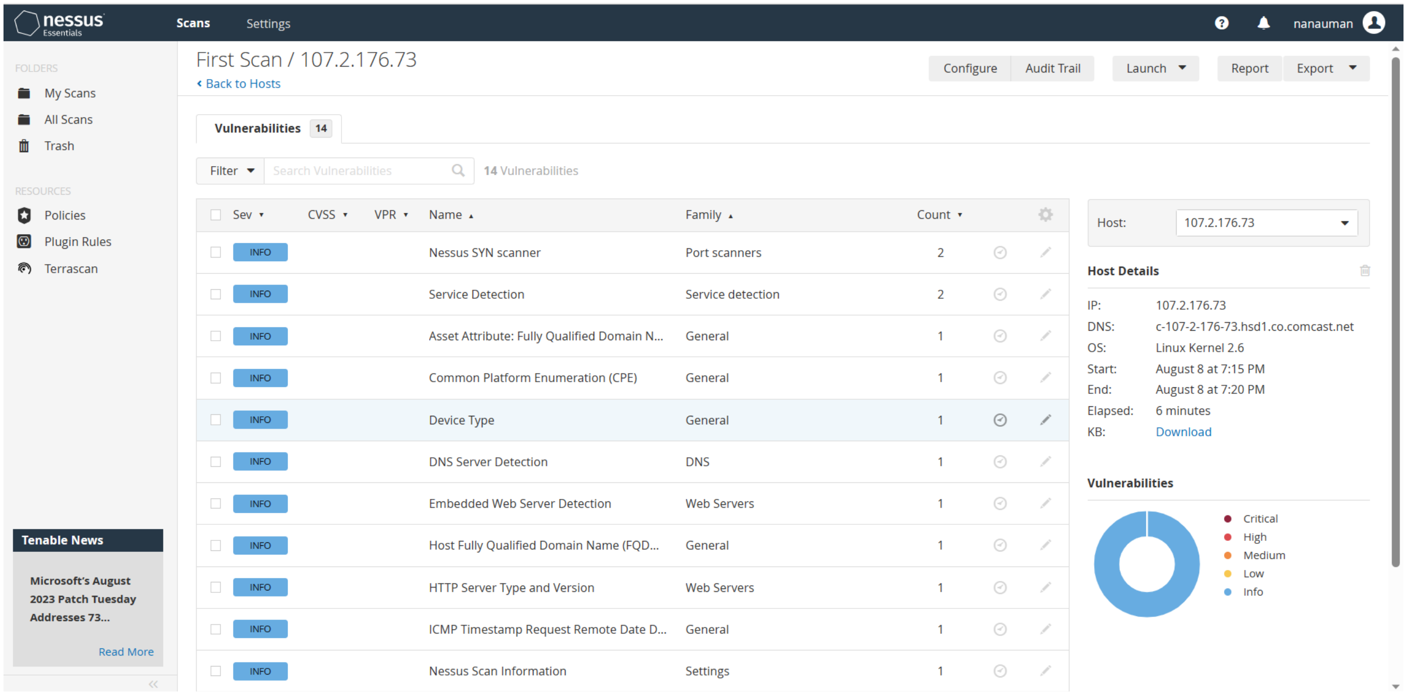


```
 ----------------------------------------------------------------------

 GRC Port Authority Report created on UTC: 2023-08-06 at 01:43:55

 Results from scan of ports: 0, 21-23, 25, 79, 80, 110, 113,
                             119, 135, 139, 143, 389, 443, 445,
                             1002, 1024-1030, 1720, 5000

     1 Ports Open
     1 Ports Closed
    24 Ports Stealth
 ---------------------
    26 Ports Tested

 The port found to be OPEN was: 80

 The port found to be CLOSED was: 443

 Other than what is listed above, all ports are STEALTH.

 TruStealth: FAILED - NOT all tested ports were STEALTH,
                    - NO unsolicited packets were received,
                    - NO Ping reply (ICMP Echo) was received.

 ----------------------------------------------------------------------
```

Press your browser's BACK bu



```
----------------------------------------------------------------------

GRC Port Authority Report created on UTC: 2023-08-06 at 02:00:26

Results from scan of ports: 0-1055

    2 Ports Open
    1 Ports Closed
 1053 Ports Stealth
---------------------
 1056 Ports Tested

Ports found to be OPEN were: 80, 554

The port found to be CLOSED was: 443

Other than what is listed above, all ports are STEALTH.

TruStealth: FAILED - NOT all tested ports were STEALTH,
                   - NO unsolicited packets were received,
                   - NO Ping reply (ICMP Echo) was received.

----------------------------------------------------------------------
```



First Scan / 107.2.176.73

‹ Back to Hosts

Vulnerabilities 14

14 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
INFO			Nessus SYN scanner	Port scanners	2
INFO			Service Detection	Service detection	2
INFO			Asset Attribute: Fully Qualified Domain N...	General	1
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	General	1
INFO			DNS Server Detection	DNS	1
INFO			Embedded Web Server Detection	Web Servers	1
INFO			Host Fully Qualified Domain Name (FQD...	General	1
INFO			HTTP Server Type and Version	Web Servers	1
INFO			ICMP Timestamp Request Remote Date D...	General	1
INFO			Nessus Scan Information	Settings	1

Host: 107.2.176.73

Host Details

IP:	107.2.176.73
DNS:	c-107-2-176-73.hsd1.co.comcast.net
OS:	Linux Kernel 2.6
Start:	August 8 at 7:15 PM
End:	August 8 at 7:20 PM
Elapsed:	6 minutes
KB:	Download

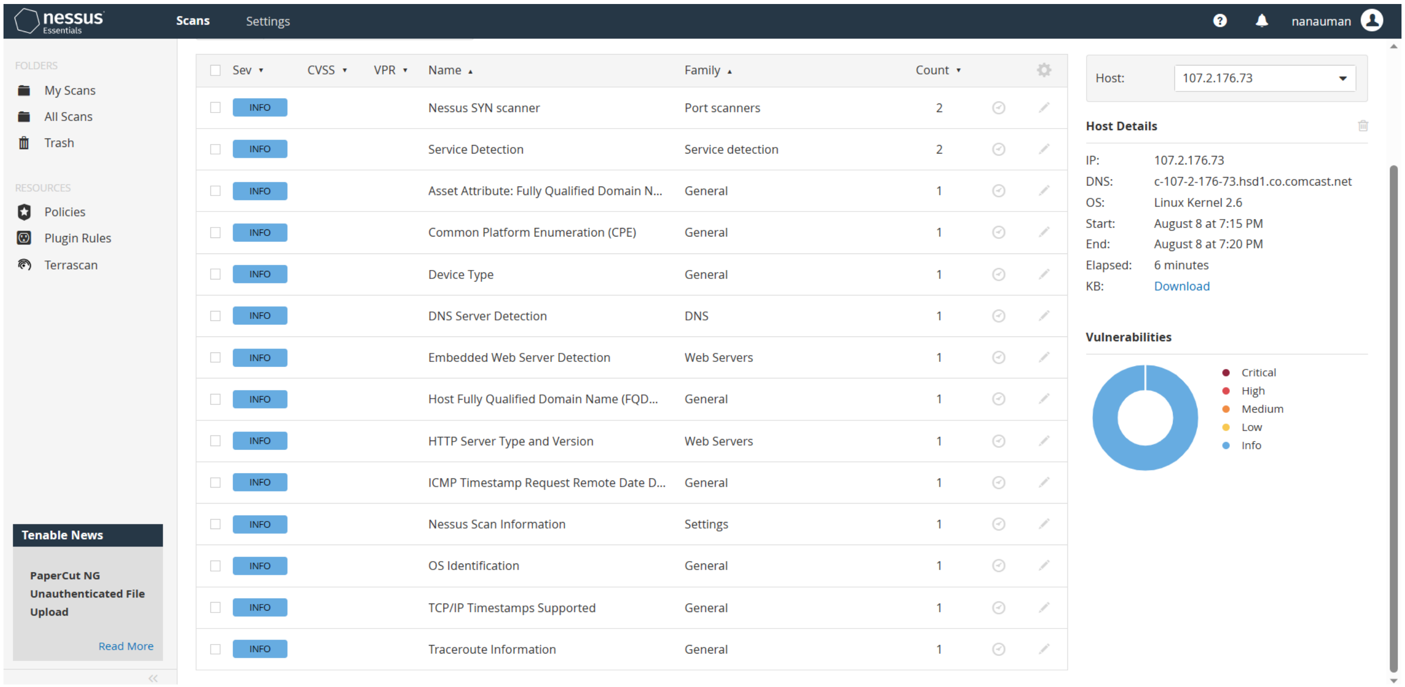
Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

Tenable News

Microsoft's August 2023 Patch Tuesday Addresses 73...

Read More



Sev	CVSS	VPR	Name	Family	Count
INFO			Nessus SYN scanner	Port scanners	2
INFO			Service Detection	Service detection	2
INFO			Asset Attribute: Fully Qualified Domain N...	General	1
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	General	1
INFO			DNS Server Detection	DNS	1
INFO			Embedded Web Server Detection	Web Servers	1
INFO			Host Fully Qualified Domain Name (FQD...	General	1
INFO			HTTP Server Type and Version	Web Servers	1
INFO			ICMP Timestamp Request Remote Date D...	General	1
INFO			Nessus Scan Information	Settings	1
INFO			OS Identification	General	1
INFO			TCP/IP Timestamps Supported	General	1
INFO			Traceroute Information	General	1

Host: 107.2.176.73

Host Details

IP:	107.2.176.73
DNS:	c-107-2-176-73.hsd1.co.comcast.net
OS:	Linux Kernel 2.6
Start:	August 8 at 7:15 PM
End:	August 8 at 7:20 PM
Elapsed:	6 minutes
KB:	Download

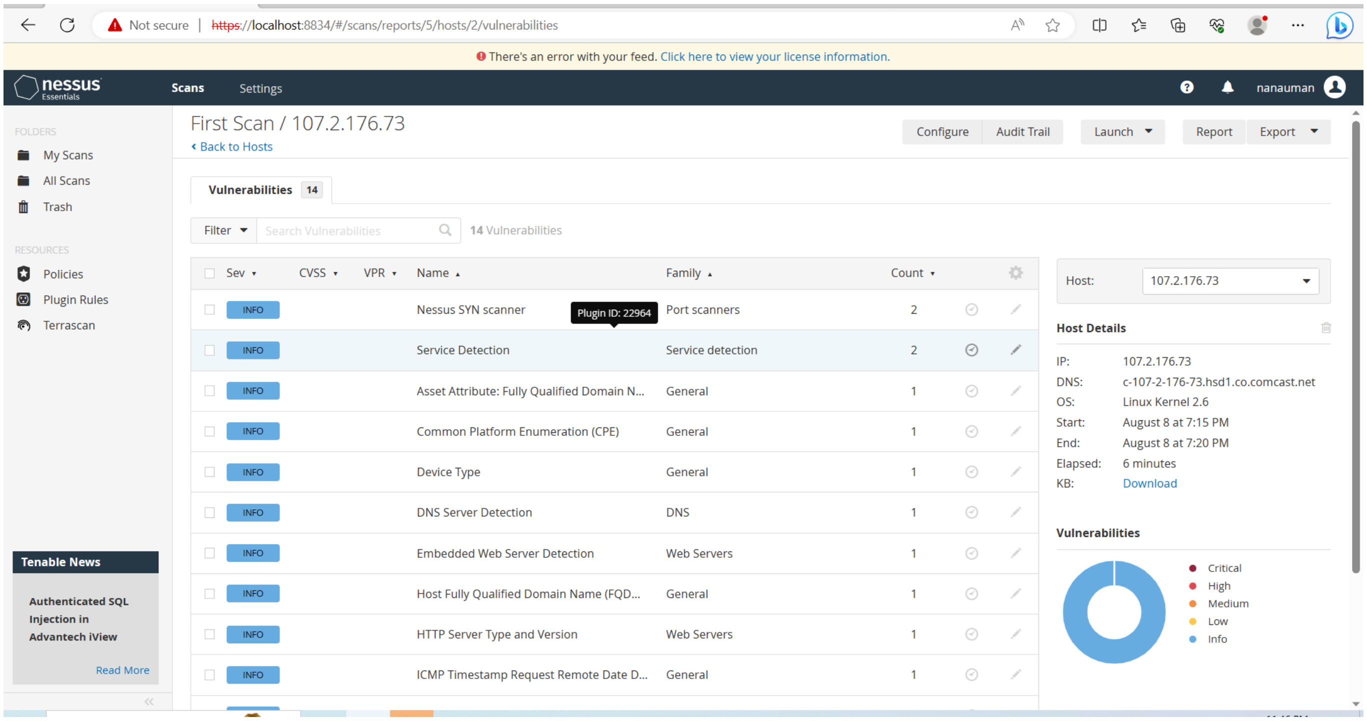
Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

Tenable News

PaperCut NG Unauthenticated File Upload

Read More



Not secure | https://localhost:8834/#/scans/reports/5/hosts/2/vulnerabilities

There's an error with your feed. Click here to view your license information.

Tenable News

Authenticated SQL Injection in Advantech iView

Read More

First Scan / 107.2.176.73

‹ Back to Hosts

Vulnerabilities 14

14 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
INFO			Nessus SYN scanner	Port scanners	2
INFO			Service Detection	Service detection	2
INFO			Asset Attribute: Fully Qualified Domain N...	General	1
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	General	1
INFO			DNS Server Detection	DNS	1
INFO			Embedded Web Server Detection	Web Servers	1
INFO			Host Fully Qualified Domain Name (FQD...	General	1
INFO			HTTP Server Type and Version	Web Servers	1
INFO			ICMP Timestamp Request Remote Date D...	General	1

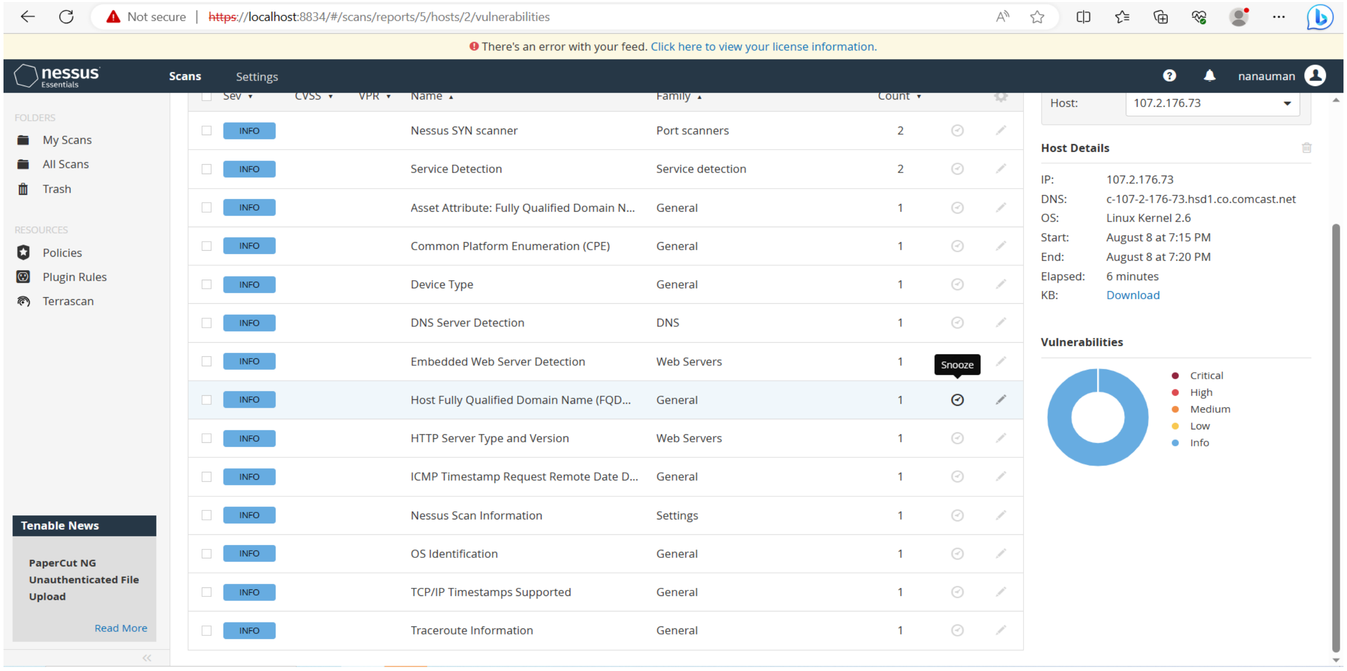
Plugin ID: 22964

Host: 107.2.176.73

Host Details

IP: 107.2.176.73
DNS: c-107-2-176-73.hsd1.co.comcast.net
OS: Linux Kernel 2.6
Start: August 8 at 7:15 PM
End: August 8 at 7:20 PM
Elapsed: 6 minutes
KB: Download

Vulnerabilities



Not secure | https://localhost:8834/#/scans/reports/5/hosts/2/vulnerabilities

There's an error with your feed. Click here to view your license information.

Tenable News

PaperCut NG Unauthenticated File Upload

Read More

Sev	CVSS	VPR	Name	Family	Count
INFO			Nessus SYN scanner	Port scanners	2
INFO			Service Detection	Service detection	2
INFO			Asset Attribute: Fully Qualified Domain N...	General	1
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	General	1
INFO			DNS Server Detection	DNS	1
INFO			Embedded Web Server Detection	Web Servers	1
INFO			Host Fully Qualified Domain Name (FQD...	General	1
INFO			HTTP Server Type and Version	Web Servers	1
INFO			ICMP Timestamp Request Remote Date D...	General	1
INFO			Nessus Scan Information	Settings	1
INFO			OS Identification	General	1
INFO			TCP/IP Timestamps Supported	General	1
INFO			Traceroute Information	General	1

Snooze

Host: 107.2.176.73

Host Details

IP: 107.2.176.73
DNS: c-107-2-176-73.hsd1.co.comcast.net
OS: Linux Kernel 2.6
Start: August 8 at 7:15 PM
End: August 8 at 7:20 PM
Elapsed: 6 minutes
KB: Download

Vulnerabilities