



nemasis

**Passive
Vulnerability
Scanner**

Product Version: 14.0.1000.118

Document Version: NVA-PVS-1404

What is Passive Vulnerability Scanner?

The Passive Vulnerability Scanner (PVS) continuously monitors the activity of endpoints, ports, applications, databases, servers and networking devices connected across network to determine its vulnerabilities in a non-intrusive manner. The PVS also informs if any software attempts to act as a backdoor for hackers or Trojans, which ports are open, the data being sent to, from and within, the services being run and the parts of system vulnerable to security threats.

The Nemasis PVS monitors all network traffic on real-time basis and alerts user to malicious asset activity. It detects and profiles all devices that connect to the network (even those that are difficult to scan, corporate owned). After scanning all the data and events are sent to the server (Syslog, SIEM, or eScan) as and when they occur for centralized analysis, monitoring, and custom reporting.

Why an organization needs PVS?

While an Active Vulnerability Scanner (AVS) ensures your assets and the applications running on it are equipped with latest patches to prevent network breaches, the PVS ensures your network security to prevent any vulnerabilities/intrusions within or outside the network.

Since an Active Scanner has to communicate with a target system by sending and receiving data packets it faces physical limitations of networks and systems. Also, if Active Scanner is scanning a network of large scale, looking out for all vulnerabilities is bound to take huge amount of time.

In few rare scenarios, a target system may even become instable after a vulnerability scan. Also, if you are including the switches and routers in vulnerability scans, they may also get affected by target system enumeration and port scans. And while we are at it, let's not forget about the network changes happening due to countless reasons.

While the small medium businesses are open minded for vulnerability scans, same cannot be said for big enterprises. Due to the large number of systems and the important information they contain, a lot of IT administrators do not want to make any compromise. Well, such a huge risk can be compensated by deploying a Passive Scanner to monitor these networks and find the vulnerabilities.

How does PVS work?

The work operation of the PVS is explained in following points:

Network Monitoring

The PVS monitors a network's vulnerabilities by carrying out a direct analysis of the data packets it sends and receives. In a way, the PVS functions just like Intrusion Detection System (IDS) i.e. it *sniffs* the traffic and informs about malicious activities. To ensure the PVS works finely on your network, deploy it on a network tap, hub or a mirrored port of a switch.

Service Identification and Passive Topology

When a target system uses network, it emits SYN packets. Every Operating System (OS) builds their SYN packets in a different manner. By monitoring these SYN packets, the PVS identifies the exact OS. The PVS also uses various techniques to determine the host type and whether it is active or not.

The PVS monitors the network traffic and builds a network structure of the active hosts on the network and the services they are running. For example, the PVS will monitor the TCP port 25 SYN packets from an active host, determine if the gathered information is new and then reevaluate the network structure.

Simple Banner Analysis

By using the specific network plugins, PVS identifies vulnerable service banners, rebuilds both sides of a network conversation and analyzes the gathered data for server or client vulnerabilities. Different servers and clients use different protocols like FTP, SMTP and HTTP. These protocols have their own unique strings and can be identified by PVS easily along with their version number.

Intelligent Banner Analysis

The PVS's vulnerability detection is capable of more than just matching banner plugins. A lot of complex protocols like SNMP and DNS need logic and many steps to identify a client's or underlying service's current version. To effectively carry out such heavy tasks, the PVS is loaded with a plugin language containing "regex" styles of pattern matching. In few scenarios, new plugins can also be written by monitoring the protocols.

Traffic Dependency

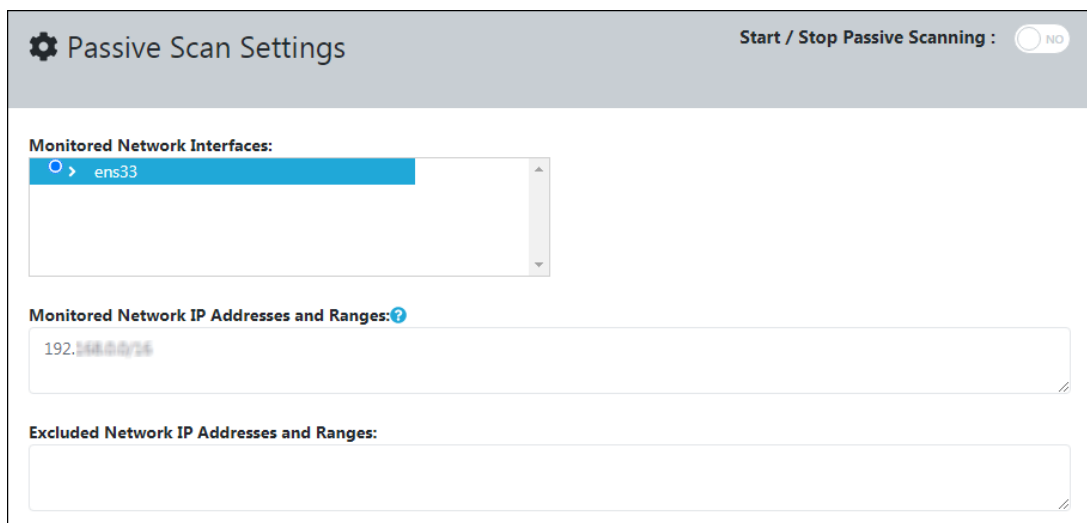
To provide an accurate result about vulnerability, PVS needs to monitor the data packet. If a server does not communicate, it will not be identified by PVS. In scenarios where an AVS can't be used, PVS will make for an excellent replacement. Furthermore, it is considered a good practice to carry out passive scans in between active scans.

The Nemasis PVS module contains following submodules:

- Settings
- Activity Monitor
- Host
- Country
- Vulnerabilities

Settings

The Settings submodule lets you configure Passive Scanner according to your network. Refer to Figure 1.



The screenshot shows the 'Passive Scan Settings' configuration window. At the top right, there is a toggle switch for 'Start / Stop Passive Scanning' which is currently turned off (labeled 'NO'). Below this, the 'Monitored Network Interfaces' section features a dropdown menu with 'ens33' selected. The 'Monitored Network IP Addresses and Ranges' section has a text input field containing '192.168.0.0/24'. The 'Excluded Network IP Addresses and Ranges' section is currently empty.

Figure 1

Start/Stop Passive Scanning

Click the toggle to start/stop the passive scanning of devices connected across the network.

Monitored Network Interfaces

A network interface is a hardware or software interface between two pieces of equipment or protocol layers in a computer network. This field will display the network interfaces discovered on the Nemasis installed system. To monitor the data traffic, ensure that at least a single network interface is selected.

Clicking the anchor displays the network interface's details. Refer to Figure 2.

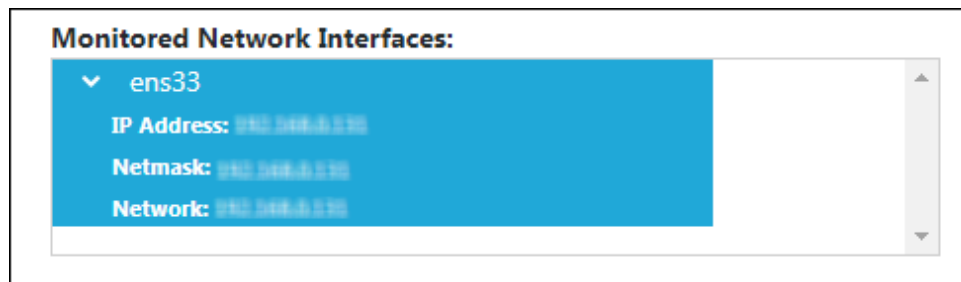


Figure 2

Monitored Network IP addresses and Ranges

Enter the IP addresses or ranges to be continuously monitored for passive scanning. You can enter the IP address in the field with following formats:

- Single IP address, for example 192.168.25.151
- IPv4 address range, for example 192.168.25.151-251
- IPv4 network in CIDR notation, for example 192.168.25.0/24
- Multiple IP addresses separated by commas

To monitor a VLAN network, ensure you are using the syntax **vlan ipaddress/subnet**.

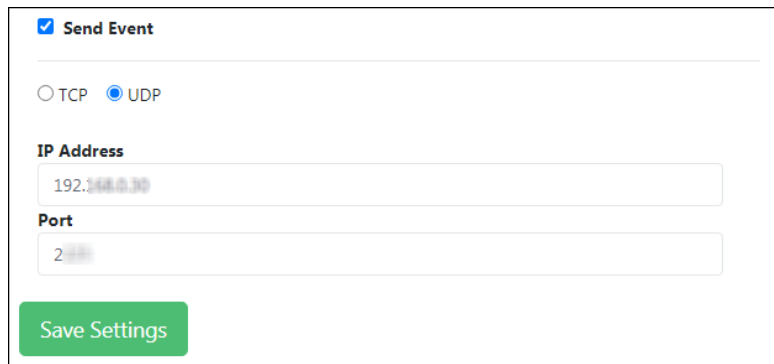
Excluded Network IP Addresses and Ranges

Enter the specific IP addresses or ranges to be excluded from passive scanning. You can enter the IP address in the field with following formats:

- Single IP address, for example 192.168.25.151
- IPv4 address range, for example 192.168.25.151-251
- IPv4 network in CIDR notation, for example 192.168.25.0/24
- Multiple IP addresses separated by commas

To exclude a VLAN network, ensure you are using the syntax **vlan ipaddress/subnet**. If this field is left blank, all IP addresses will undergo passive scan.

Nemasis allows you to configure Nemasis PVS to forward events in clear text format on real-time basis to a syslog, SIEM, or eScan server. Refer Figure 3.



Send Event

TCP UDP

IP Address
192.168.0.30

Port
2

Save Settings

Figure 3

Send Event

The PVS allows you to send events to a Syslog, Security Information and Event Management (SIEM), or eScan server. You can configure it via following options:

TCP/UDP: Select the transfer protocol (TCP or UDP).

IP Address: Enter the IP Address of the receiving SIEM server.

Port Number: Enter the listening port number on the SIEM server.

After making changes, click **Save Settings**. The Passive Scanner will scan the network as per the new settings.

NOTE	Nemasis PVS will still record the security and system events and display them in reports in the Nemasis Console even if you enable event forwarding to a syslog, SIEM, or eScan server.
-------------	---

Activity Monitor

The Passive Scanner monitors the data packets in a network. The Activity Monitor displays the analyzed network traffic information in the form of a dynamic graph. Refer to Figure 4.

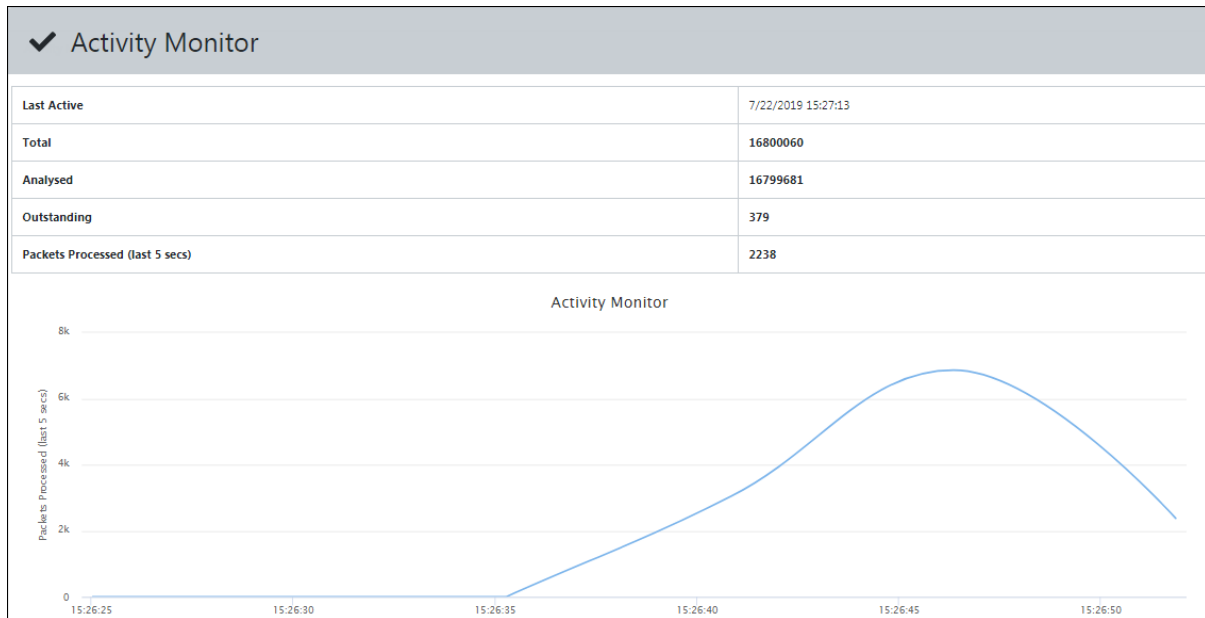


Figure 4

Last Active

It displays the last active status of the Passive Scanner in local date and time.

Total

It displays the total number of data packets.

Analyzed

It displays the number of data packets analyzed by the Passive Scanner.

Outstanding

It displays the number of data packets that are yet to be analyzed by the Passive Scanner.

Packets Processed (Last 5 secs)

It displays the number of data packets processed in last five seconds by the Passive Scanner.

Host

The Host submodule displays a list of IP addresses, its country of origin and a stacked bar chart that is labeled and color coded to define the number of vulnerabilities and its severity level. Refer to Figure 5.

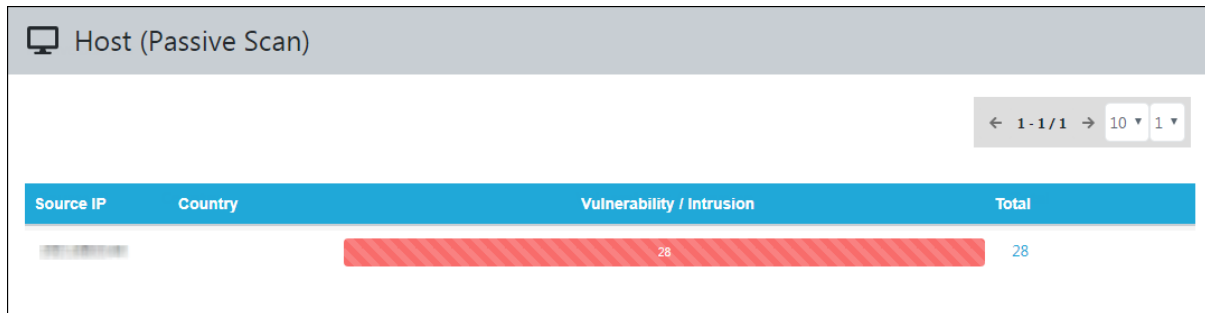


Figure 5

Source IP

This column displays the IP address of endpoint sending malicious data packets to other endpoints connected across the network.

Country

This column displays the country of origin of the public IP address. Users should note that country will be displayed only for public IP addresses.

Vulnerability/Intrusion and Total

Clicking the Vulnerability/Intrusion chart or numerical value in Total column displays the vulnerability's name and total number of malicious attempts made by it. Refer to Figure 6.

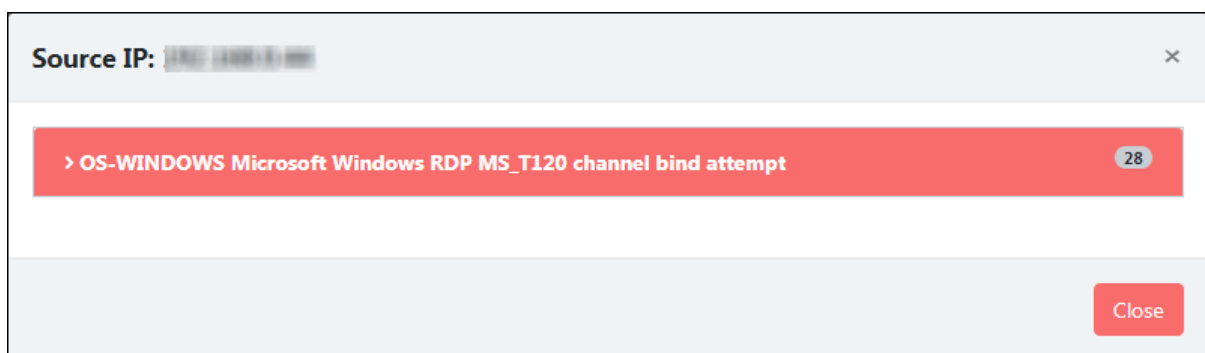


Figure 6

Clicking the vulnerability displays following details. Refer to Figure 7.

- The vulnerability's first and last observation by passive scanner.
- References for the vulnerability.
- Ports from which the malicious data packets were sent to the destination IP addresses and Port number.

Source IP: [redacted]

OS-WINDOWS Microsoft Windows RDP MS_T120 channel bind attempt 28

First Observed: Jul 03 2019 12:11 PM Last Observed: Jul 03 2019 12:11 PM

See References

<http://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0708>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-0708>

59703/TCP	→	[redacted]:3389
59705/TCP	→	[redacted]:3389
59745/TCP	→	[redacted]:3389
59736/TCP	→	[redacted]:3389
59822/TCP	→	[redacted]:3389

Show More...

Close

Figure 7

Country

The Country submodule displays the country of intrusive public IP address, vulnerability/intrusion bar and total number of times it sent malicious data packets. Refer to Figure 8.

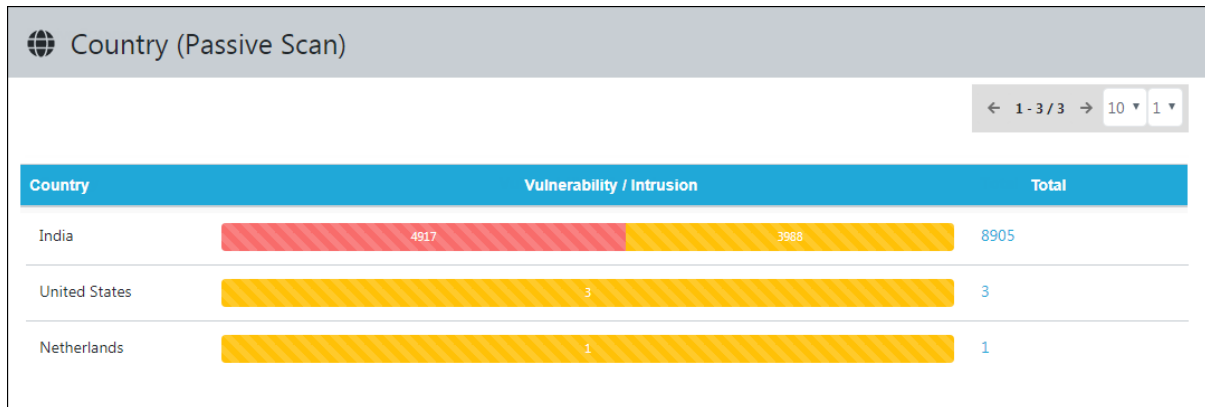


Figure 8

Vulnerability/Intrusion

Clicking the bar chart displays the list of public IP addresses and total number of malicious attacks attempted. The different sections in bar will display different findings. For example, clicking the Red section of the India's bar chart displays only the Red section's findings. Refer to Figure 9.

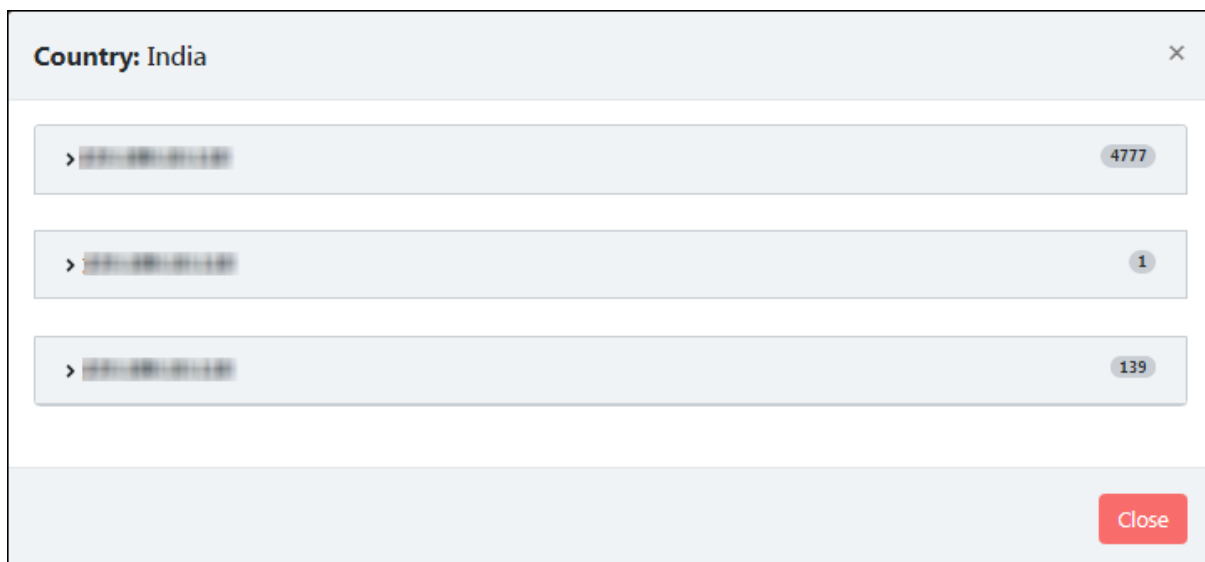


Figure 9

Clicking the IP address field further displays the vulnerability, first and last observation, references, source Port number, destination IP address and Port number. Refer to Figure 10.

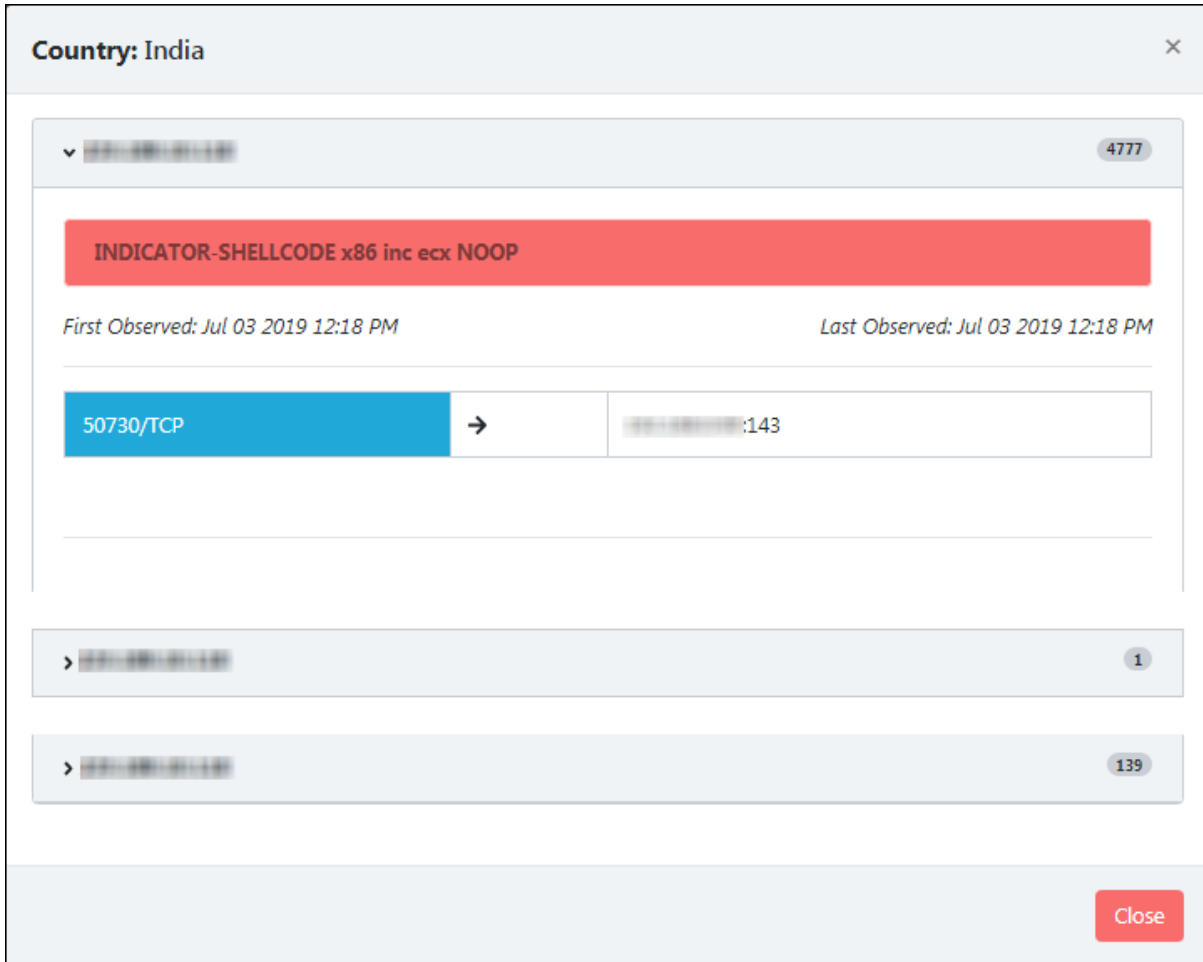


Figure 10

Total

Clicking the numerical value in Total column displays a list of public IP addresses and malicious attacks attempted by them.

Vulnerabilities

The Vulnerabilities submodule displays the vulnerabilities detected in descending order of severity. It also displays vulnerability's name, its first and last observation, references and total number of times it sent malicious data packets. Refer to Figure 11.

Vulnerabilities (Passive Scan)

← 1 - 8 / 8 → 10 1

Vulnerability / Intrusion	First Seen	Last Seen	References	Total
INDICATOR-SHELLCODE x86 inc ecx NOOP	Jul 03 2019 06:48 AM	Jul 03 2019 07:10 AM	0	3260
OS-MOBILE Android User-Agent detected	Jul 03 2019 06:57 AM	Jul 03 2019 07:08 AM	0	4
INDICATOR-SHELLCODE ssh CRC32 overflow filler	Jul 03 2019 06:50 AM	Jul 03 2019 07:05 AM	3	4
OS-WINDOWS Microsoft Windows RDP MS_T120 channel bind attempt	Jul 03 2019 06:41 AM	Jul 03 2019 06:41 AM	2	30
PROTOCOL-IMAP login brute force attempt	Jul 03 2019 06:47 AM	Jul 03 2019 07:10 AM	1	1621
PROTOCOL-IMAP fetch overflow attempt	Jul 03 2019 06:47 AM	Jul 03 2019 07:07 AM	3	98
PROTOCOL-IMAP append literal overflow attempt	Jul 03 2019 06:47 AM	Jul 03 2019 07:10 AM	3	1340
POLICY-OTHER Microsoft Windows Terminal server request attempt	Jul 03 2019 06:48 AM	Jul 03 2019 07:10 AM	6	29

Figure 11

References

Clicking the numerical value in References column displays various references for the vulnerability. Refer to Figure 12.

References: INDICATOR-SHELLCODE ssh CRC32 overflow filler

See References

- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0572>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0144>
- <http://www.securityfocus.com/bid/2347>

Close

Figure 12

Total

Clicking the numerical value in Total column displays the IP addresses and total number of times malicious data packets sent. Refer to Figure 13.

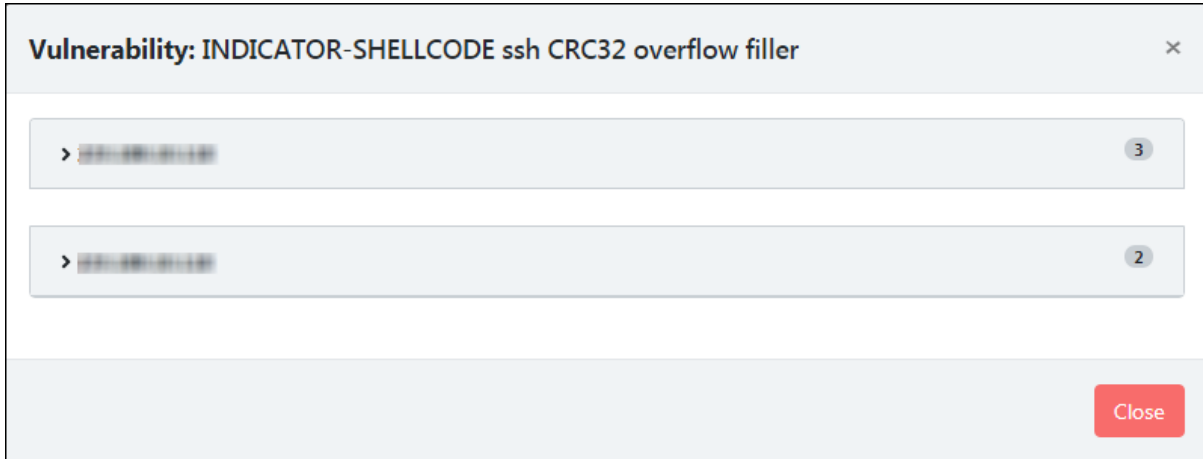


Figure 13

Clicking the IP address field further displays the source Port number, destination IP address and Port number. Refer to Figure 14.

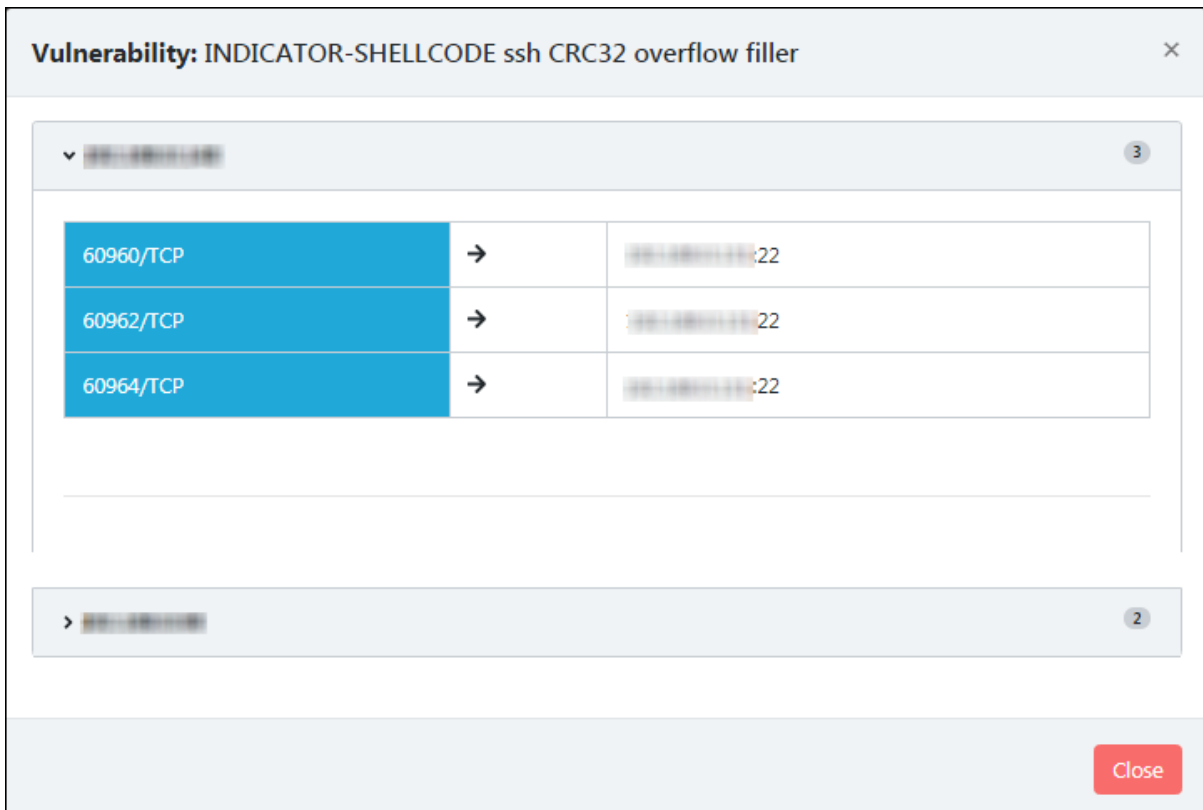


Figure 14