LSN Documents Documentation

Ajinkya Wadekar

Apr 03, 2019

Contents:

We are a Dedicated and Cloud Hosting company. Here you will find information about most of the technologies we use in managing our infrastructure. We use Openstack for our cloud, Ansible for orchestration etc.

CHAPTER 1

Guide

1.1 Limestone Addon Services

1.1.1 DDoS Protection

1.1.2 DNS rDNS

1.1.3 KVMoIP

1.1.4 NAS

1.1.5 Software

1.1.6 SSL Certificates

1.1.7 VPN

1.1.8 General

1.2 OnePortal

1.3 Operating System Support

1.3.1 Linux Support

1.3.2 Windows Support

1.4 Abuse

1.4.1 Malicious Network Traffic

Why am I receiving this notification?

An abuse ticket will automatically be opened on your account when Limestone Networks has received an abuse report for an IP address currently assigned to your server.

What is Malicious Network Traffic?

Limestone Networks considers Malicious Network Traffic as any of the following:

Port Scanning

An attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service.

Malicious HTTP GET/POST requests

An attack against a web server to discover commonly used scripts or software, with the goal of exploiting a known vulnerability in that software.

Any type of unauthorized brute-force attack against another server

An attack used for trying many combinations of standard or frequently used username and passwords (e.g.: root/password). These attacks are commonly directed towards SSH and RDP services.

Why is my server sending out malicious network traffic?

This type of activity typically occurs because a malicious script or program was installed on the server. This may have been due to a compromise of the server's security or by a user granted access to your server.

Common Attack Vectors

- Login credentials have been brute forced or compromised
- User visited a malicious website and malware was installed without their knowledge
- A vulnerability in website software allowed the attacker to upload a malicious script
- A user knowingly installed malicious scripts/software on the server.

How can I identify the script or software responsible?

If your operating system is Linux we suggest using the "ps" command to view the running processes on the system.

How to show all running processes in Linux

If your operating system is Windows we suggest downloading and running Process Explorer from Microsoft. Process Explorer is a more advanced version of Windows Task Manager. You can use this program to help identify processes running on your system that you do not recognize. You can also find where on your system a process is running from and what connections to the internet it is making.

Download Process Explorer

Resources:

http://en.wikipedia.org/wiki/Port_scanner http://en.wikipedia.org/wiki/Brute-force_attack http://lasamhna.de/library/brutessh.html

1.5 LSN Cloud CDN

1.5.1 Cloud Solutions

1.5.2 Content Delivery Networks

1.6 Resellers

1.7 TOS AUP

CHAPTER 2

Indices and tables

- genindex
- modindex
- search