Automation in Network Security

1Om Khard, 2Deepak Kahar, 3Akshansh Joshi, 4Omkar Singh
Student
Jain University

Abstract **- The Automation in Network Security is a backend Server Side Application Project which uses Automation and OSINT using Python to detect any malicious , compromised , unsanitized , and unknown data formatted to be transferred or requested to a Server . It is a kind of statefull Firewall in a way which uses Automation and Telemetry Techniques to determine any malicious , harmfull , unsanitized requests and then blocks it to allow to the network . This idea is to make Web and Internet much more a Secure Place using Authentication , Sanitisation , Packet Inspection , Authorisation etc.**

keywords **- Firewall , Network Automation , Python and JSON**

Introduction

We know that Automation is Future , and in a world where everything and everybody is connected with a 'web' or devices It becomes a responsible task to make the cyber place Secure . So we came up with the Idea to use Automation in Network Security using OSINT .

- First we will inspect each and every packet coming to the server .
- Then we will use OSINT to detect what are the specialities and recommendation for a malicious data format from SNORT IDS .
- Using OSINT policies we will allow and block the data after being checked from our Firewall .
- Osint is a technique for gather and inspecting data in an automation way.

Literature Survey

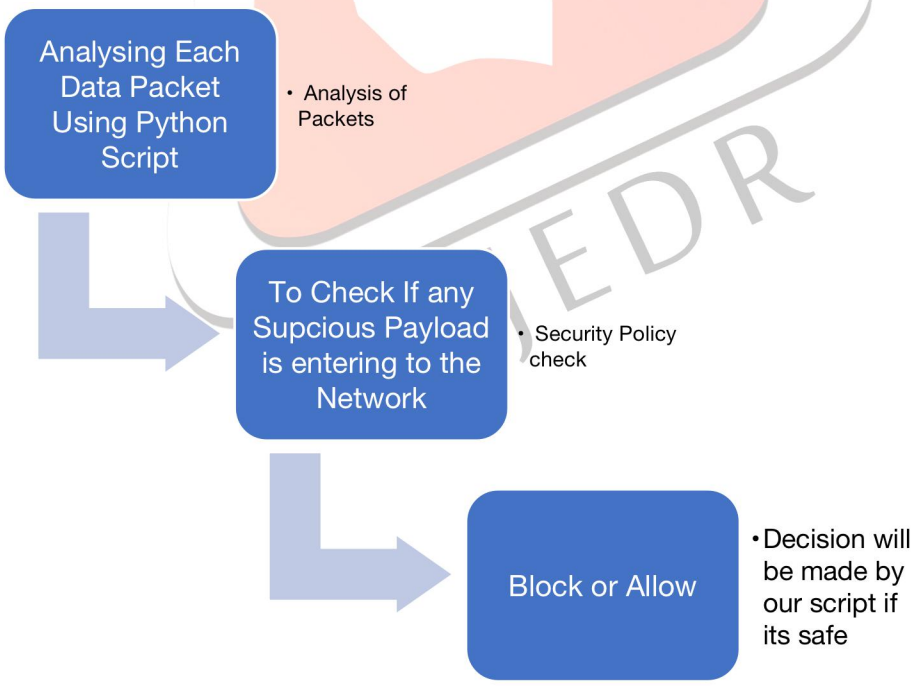
Publication year	Title	Overview	Positive Aspects	Limitations Overcome
CORSA , 2021	Automating Firewall Virtualisation	Current firewall architectures are complicated, do not scale and lock you in. That's why many people are looking at virtualization to solve the issue just like it did for data centers and the cloud .	It promotes virtualization	It adds more weight and parameters for public cloud uses and virtualistation
Snort , 2020	The Snort Project	This manual is based on Writing Snort Rules by Martin Roesch and further work from Chris Green	Snort really isn't very hard to use, but there are a lot of command line options to play with,	It is an IDS uses terminal or graphical interface for intrusion detection
PaloAlto Networks , 2021	The DevSecGuide to Infrastructure as Code	DevSecOps has paved the way for teams to automate security and embed it into the DevOps lifecycle.	The rise of IaCInfrastructure as code—also known as IaC—was first introduced in 2009 by DevOps company Puppet in response to the traditional methods of deploying and managing infrastructure.	It introduces to the word IaaC (Infrastructure as a Code), DevSecOps which are the future in Cyber Security
OWASP OSINT , by Adam Nurudini 2020	OSINT OPEN-SOURCE INTELLIGENCE OSINT	What is OSINT • Collect data indirectly without knowing other information	Open-Source Intelligence (OSINT) is intelligence collected from public available sources	TYPES OF OSINT From Security perspective we can separate OSINT into:

		• Collect data about servers, location, operating systems, etc. • Threat intelligence for your organization • Data gathering that could protect you and your company • Skills of GHDB • Shodan methods and operations • OSINT using free tools only	"Open" refers overt, public available sources (as opposed to covert sources) Its not related to open-source software or public intelligence This information comes from a variety of sources, including the social media pages of your company and staff. These can be a goldmine of information, revealing information such as the design of ID badges, layout of the buildings and software used on internal systems.	•Offensive: Gathering information before an attack •Defensive: Learning about attacks against the company.

Objectives

- Our Idea is for Cyber Security Solutions , and protecting a network of either a Server side or a host side from any malicious file transfer , or any Cyber Threat .
- We analyse each packet of data coming to a server or any host , if any suspicious encapsulation or payload exist our Firewall just eventually blocks it from the entire network to get affected .
- We use OSINT (Open Source Intelligence) to judge which is suspicious and malicious at the same time when running our Python Script provided by SNORT IDS .
- It is to secure a Company's Network whenever there comes any intrusive request to there server or network .

Methodology



Hardware and Software Requirements

Hardware Requirements

1. CPU intel CORE i5 5th gen or higher .
2. Cores minimum dual Core .
3. Hard Disk to be higher than 250GB .
4. RAM of minimum 4GB.

Software Requirements

1. Python 3.x
2. Modules like socket , requests , urllib3 , struct , should be preinstalled
3. Linux of any distro (Only for Linux)
4. A Good Internet Connection to make it safe