International Journal of Allied Practice, Research and Review

Website: www.ijaprr.com (ISSN 2350-1294)

ANSIBLE: Automating Network Security

Ritika Verma[1], Opel Nahar[2] and Anand Sharma[3]
CSE Department, CET-MUST,
Lakshmangarh, Sikar, Rajasthan, India

Abstract - It is impossible to be isolated from the Internet. And with it, comes Security threats that are real. The basic aspects of information must be protected. Network Security deals with the use of cryptographic algorithms in network protocols and network applications i.e, it consists of the measures to protect data during their transmission. Ansible looks forward to the automation of even the most complex multi-tier application ITenvironments. It is a tool that can be used by developers, operations, and security teams alike. Security being a necessary integral component, we look forward to Ansible in automating Network Security.Ansible is a great tool for Security Automation.In this paper, first we discusses about Ansible, then Network Security and finally at the last we will describe Automating Network Security using Ansible.

Keywords - ***Ansible, Network Security, Automation, Cryptography, Encryption, Decryption*****.**

I. Introduction

Ansible is a very simple tool that can be used and loved by developers, operations, and security teams alike. Simple yet it is powerful enough to automate even the most complex multi-tier application IT environments.

Some key features of Ansibleare: It is Simple, Agentless, Efficient, Powerful and flexible. It uses simple syntax written in YAML called as playbooks that are very easy to write. One who doesn't even know what Ansible is can likely read a playbook and understand what is happening. Common Ansible use cases are: Configuration Management, Continuous Integration / Delivery, Orchestration, Infrastructure Provisioning, Application Deployment and Security Automation. Ansible for security and compliance: When security policy is defined in Ansible, scanning and remediation of site-wide security policy can be integrated into other automated processes. And it'll be integral in everything that is deployed. Moreover, all the credentials (admin user's id's & passwords) that are stored within Ansible are not retrievable in plain-text by any user.

Ansible can be thanked for helping to successfully bridge the gap between Devs and SystemAdmins, for not using XML, for powerful ad-hoc, reusable one-liners, for not having a

DSL, for a gentle learning curve and fast getting-started process, for not using agents or daemons on custom ports, for offering idempotence and helpful dry-runs, for continuously expanding and improving the support for cloud providers (esp. AWS).

Ansible allows to simply defining systems for security. Ansible's easily understood Playbook syntax allows to secure any part of the system, whether it's setting firewall rules, locking down users and groups, or applying custom security policies. Ansible comes with a library of over 750 included automation modules, allowing to quickly perform tasks without complicated scripting and Ansible's easily reusable roles lets us write the automation procedures once and use them across the entire infrastructure. Plus, when the need arrives to perform a one-off task like quickly applying a security patch from a vendor, Ansible's command support allows getting things done across the infrastructure with one simple command.

II. Network Security

Network Security deals with the use of cryptographic algorithms in network protocols and network applications. Security aims at controlling data / network accesss, preventing intrusions, responding to incidences, ensuring network availability and protecting information in transit. Cryptography is the study of methods for secret writing, transforming messages into unintelligible form, recovering messages using some secret knowledge.

Encryption holds utmost importance as it plays a very important role in protecting information. It is the process of transforming plaintext to ciphertext using a cryptographic key (secret key). Decryption is transforming ciphertext back to original plaintext.

A common conceptual model of security practices, the CIA Triad, focuses on three aspects of
(Primarily data) protection:

Fig. 1 CIA Triad

- Confidentiality

  Preventing unauthorised use or disclosure of any information.

- Integrity

  Ensuring that data has not been altered or deleted by an unauthorized partyi.e it safeguards the accuracy and completeness of information.

- Availability

  Ensuring that data will be available when it's needed and the users that are authorised will have reliable and timely access to information.

Moving towards using automation as part of IT practices is a necessary first step for security. The proper automation tooling allows applying the security you need in a simple, consistent, manner, allowing you to concentrate on other things.

As of now, for information security, it is required to or it must adapt to a changing scenario. Be it providing the customersand partners with permission to access certain systems and data, permitting the employees so as to use their own phones(smartphones) and laptops, working using applications from Software-as-a-Service (SaaS) sellers, or taking or gaining the benefit of 'pay-as-you-go' utility pricing models by public cloud providers. Making the most productive utilization of a firm's information assets may need sharing that information with only the permitted third parties. Both the aspects, regulatory agreement and the total
power and sophistication ofthe cyber-attacks emphasizes the requirement for an IT security planning that works better and is moremultifarious than the conventional one in almost all the organizations.

III. Automating Network Security

There are ways of Automation because it is such a crucial task in the present scenario. Almost everything in today's world, especially in the IT environment is automated and also because there are a lot of automation challenges in the market.At present we are using the following the following approaches for the same.

1. Per-application firewall rule set

   • Easy to manage, understand and audit

   • Ruleset lives and dies with the application

   • Stale rules in central firewall are gone

2. Standardize rule sets

   • Applications are not as special as their owners think

   • Create a standard ruleset for each application class

   • Changes to rule set void warranty

3. Rethink the security policy

   • Packet filters are often good enough

   • Stateful inspection is required only on links to external networks or foroutgoing sessions

The process-flow for automating network security is shown in figure 2. It has been shown that for automating first we have to simplify the thing then we the standardization is required and finally the automation part has to be done.

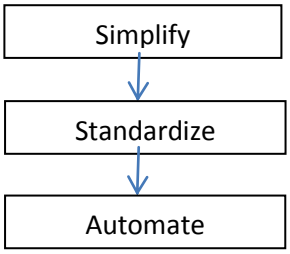

Fig. 2 Process-flow for automating network security

IV. Ansible

Automation in network security is proposed by Ansible and it works so well for it. Working on Network Security using Ansible can be a very interesting task and it can come up with the neededoutcomes. Firewall is only one entry point of the network. If Modems are allowed to answer incoming calls, it can provide an easy way to the attacker to sneak around your front door. This means that our network is required to be protected at all of its entry points.

There are some already existing Secure Network devices such as: Secure Modems, Dial-back systems, Crypto capable routers and Virtual Private Networks. Ansible can work as 'a cherry on the cake' in Network Security if used with the above stated devices.

Ansible can be used to apply and enforce security standards that adapt to meet the security guidelines for the network.

Ansibleefforttlessly runs from source and doesn't need any setup of software on remote machines, numerous users track the development version.Its launch cycles are generally of 2 months. Because of this small launch cycle, minor errors/ bugs will usually be fixed in the upcoming launch unlike keeping backports on the well-constructed branch. Considerable bugs will still have maintenancelaunchesas and when required, even though, those are not frequent.

If you wantto run the latest launched version of Ansible and you are using Red Hat Enterprise Linux (TM),CentOS, Fedora, Debian, or Ubuntu, it is suggested to use OS package manager.For other installation options, installation via "pip"is suggested, that is the Python package manager,however otheroptions are also present.It's not important to install the program to run from source.

Ansibledoes automation and orchestration of IT environments through playbooks; Playbooks are written in YAML, they can be called as YAML definition of automation jobs that relates how a specific piece of automation must be performed. As the name itself suggests, Ansible playbooks are prescriptive, but responsive descriptionsof how to carry out an operation - IT automation that genuinely explains what actually every individual aspect of your IT infrastructure requires to do, however, nonetheless lets the additives to reactto the foundinformation, and to operate with one another.

Ansibleplaybooks elucidates automation over a set of hosts, called to be the 'inventory'. Each 'play' consists of multiple 'tasks,' which could have a goal one, many, orall of the hosts within the inventory. Each and every task is a call to an Ansible module - a small piece of codefor doing a particular task. These tasks may be very easy, like placing a configuration file on atarget machine, or installing a software bundle. They can be complicated, which include spinning up an entire CloudFormation infrastructure in Amazon EC2. Ansible consists, hundreds of modules, starting from simple configuration management, to dealing with network devices, to modules forretaining infrastructure on every foremost cloud provider.

By combining different tasks into a playbook, complex automation can be achieved. As a detailed example, consider a traditional three-tier web application and its environment consisting of:

- Application servers
- Database servers
- Content servers
- Load balancers
- A monitoring system connected to an alert system

All playbooks are executed through the awx file system user. For running the jobs, Ansible Tower defaults to imparting activityisolation via Linux name spacing and chroots. This projection ensures jobs can only access playbooks and roles fromthe Project directory for that job template and common locations such as /opt. Playbooks are not able to access roles, playbooks, or data from other Projects by default.

For credential security, customers may additionally choose to upload locked SSH keys and set the unlock password to "ask". Additionally, you canalso choose to have the system prompt them for SSH credentials or pseudo passwords rather than having the system store them in the database.

Control Machine is the machine from which all the commands are ruined. Basically, using Ansible, you'll not need to give security features individually to every node or system present in the network. Just write a playbook, mention all the required security traits and run that playbook on the control machine. It will then be there at every system or node present in your network. That way, it becomes really simple to secure your network from potential threats and that too with minimum possible efforts.

Presently, Ansible runs from any machine which has Python 2.6 installed. We are having various releases for the same as follows:

- Latest Release Via Yum
- Latest Releases Via Apt (Ubuntu)
- Latest Releases Via pkg (FreeBSD)
- Latest Releases Via Homebrew (Mac OSX)
- Latest Releases Via Pip
- Tarballs of Tagged Releases

V. Conclusion

Network Security being very crucial, it would give required results if automated. Ansible could be the ideal way to achieve this, as it strives to automate no longer simply traditional IT server and software programinstallations, however the entirety of IT infrastructure, , inclusive of areas no longer blanketed with the aid oftraditional IT automation tools.

Ansible's task-based, agentless nature makes it relevant, without difficulty to the networking space, andsupport is included with Ansible for automating networking from major vendors such as Cisco,Juniper, Hewlett Packard Enterprise, Cumulus and more.

Customers looking to integrate such a sort of process process with their source control, establish a build system, or integrate with their network environment may wish to reach out to Ansible.

VI. References

[1] Red Hat, Inc., "Ansible Tower User Guide - Release Ansible Tower 3.2.1", Nov 30, 2017

[2] Jeff Geerling, "Ansible for DevOps: Server and configuration management for humans"Leanpub book, Nov 01, 2017

[3] Ansible "Ansible Documentation Release 1.7" July 14, 2014

[4] Praveen Kumar, AdityaPatawari, Ansible -Workshop DocumentationRelease 0.1", May 11, 2017

[5] Ansible Documentation: http://docs.ansible.com/ansible/

[6] Ansible Documentation: http://www.ansibleworks.com/docs/

[7] Fedora's Ansible repo: https://infrastructure.fedoraproject.org/cgit/ansible.git

[8] Introduction to Ansible Video: https://www.youtube.com/watch?v=ak4yW6mF7Ns