Network Security (Automation)

Gauri Shahane,Aditya Kshirsagar,Ashwini Gore,Sanika Jadhav

Guided by:-Mrs.N.R.Dangi

Shri Jain Vidya Prasarak Mandal's
RASIKLAL M. DHARIWAL INSTITUTE OF TECHNOLOGY
Manikchand

Abstract - The security of an operator's network is crucial while being increasingly complex to ensure. This is all the more the case with the evolution of the network towards virtualization. In this paper, we will explain how to secure a network and then give some real examples of automation implemented to ensure this security. Finally, we will detail the new risks associated with the implementation of automation tools and share some good security practices around their implementation.

Keywords : Network security automation

1.INTRODUCTION

Our lives are transformed by access to digital networks. The majority of the world's population now has mobile coverage and half of them use the Internet. Orange is one of the world's leading telecommunications network operators. We market connectivity services to individuals, companies and also wholesale for example other domestic and international operators, Internet access and content providers, etc. We use our own infrastructure: millions of kilometers of optical and copper cables, hundreds of thousands of equipment, tens of thousands of antennas and, to orchestrate the whole, thousands of technical sites and data centers. The automation of the production of equipment and services has been an important issue to respond quickly to the needs of customers and ensure a high level of quality of service. Given the exposure of the equipment and services provided by Orange, security has always been an integral part of the construction of our offers

2. Body of Paper

Network security automation can mean many different things but for us it is the practice of automatically migrating physical, or hardware, network security appliances to virtual ones and then being able to manage and scale this software-defined security for future needs. When we say network security automation, we're talking about operations which would normally be performed manually when you migrate to virtualized security —like generating an ISO image, defining VM settings, bootstrapping, provisioning—instead being implemented seamlessly without requiring DIY or custom scripts. Network security automation needs to be applied to the base of the pyramid in Deployment and Configuration first if we're to see the performance, scalability and cost savings we're looking for.

Table -1: Sample Table format
Firewall management policies:-

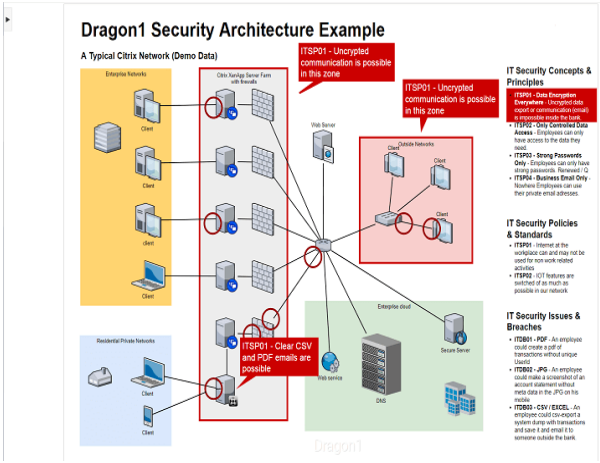
R#	prt	Source		Destination		Action
		IP_addr	port	IP_addr	port	
1	TCP	132.16.*	*	193.17.12.1	80	pass
2	UDP	*	*	193.18.*	*	deny
3	*	132.*	*	193.13.*	*	deny
4	UDP	*	*	*	*	pass
5	*	*	*	*	*	deny

Network security Testing results :-

No	Attack Techniques	Network			Tools	Description
		LAN	Wifi KOMINFO	Wifi PPID 2014		
01	Password Cracking	not success	not success	not success	Manual, aircrack-ng	Matching Password obtained from interviews to related parties
02	Network Sniffing	Success	not success	not success	Ettercap	Capture the network packets that pass through in-sniffing, such as username and password
03	Ping of Death / DDOS	Success	Success	Success	Manual, mdk3	Send package as much as possible and continuously to the network used

Fig -1: Figure

Chart



3. CONCLUSIONS

in this article we have surveyed the state of the art of the techniques for automating the configuration of network security services. After identifying how the orchestration of a full service should be performed in a virtualized environment, we focused on two different aspects, that are the design of the service architecture and the actual configuration of the composing functions. For each category, we analyzed the existing works by considering different features, such as the fulfillment of optimality criteria or the exploitation of formal verification.

ACKNOWLEDGEMENT

Network security is a broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies. Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats in the wild today.

REFERENCES

Halsall, F. (2001) *Multimedia Communications*, Addison Wesley.
ITU-T X.509 (2000) *Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks* , International Telecommunication Union.
King, T. and Newson, D. (1999) *Data Network Engineering*, Kluwer.
Peterson, L. L. and Davie, B. S. (1996) *Computer Networks: A Systems Approach*, Morgan Kaufmann.
RFC 2401 (1998) *Security Architecture for the Internet Protocol*, Kent, S., Atkinson, R.
Schneier, B. (1996) *Applied Cryptography*, 2nd edn, Wiley.
Stallings, W (1999) *Cryptography and Network Security*, Prentice Hall.
Stallings, W (2001) *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, 3rd edn, Addison Wesley.