ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 4, pp: (72-75), Month: October - December 2020, Available at: www.researchpublish.com

Automated Real-Time Detection and Security Assessment of Network Devices

Hussain Alhaddad

Saudi Aramco, Dhahran, Saudi Arabia

***Abstract*: Timely verification of security requirements for new network devices is crucial to maintain the security and protection of the enterprises' assets. This is due to the fact that insecurely configured or inadequately patched network devices deployed into a production environment may be exploited for unauthorized/malicious use. This paper will shed some light on the importance of timely security assessment against network devices and appliances and will explore the most efficient approach into addressing this requirement.**

***Keywords:* automation, network devices, appliances, security, cybersecurity, assessment, security configurations.**

I. INTRODUCTION

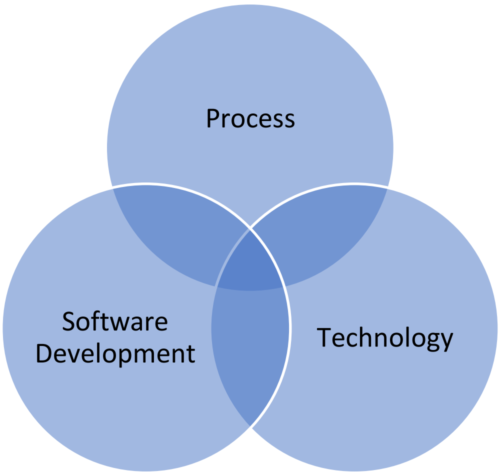
Information technology (IT) networks in organizations undergo continuous changes in terms of commissioning new devices and decommissioning existing ones. The lack of a mechanism to promptly initiate the appropriate cybersecurity actions based on the type of event (commissioning/decommissioning) would potentially increase the security risk that is posed by deploying new insecure devices. There are many types of platforms such as Windows and Linux that can host a small piece of software or agent to be part of the enterprise image. That would properly address the requirement of a timely security assessment when a new instance of these platforms is deployed into the network as the installed agent would do the job. The problem arises when new instances of systems such as network devices and appliances are deployed to the enterprise IT network as these types of systems cannot host any security agent. Therefore, the focus on network devices and appliances in this paper is meant to bridge the gap and, subsequently, elevate the cybersecurity posture of the enterprise.

The process for commissioning network devices is usually governed by systematic change management procedures where implementation tasks are assigned, tracked, and completed in a system such as Remedy. One of the methods used to ensure newly commissioned network devices are assessed from a security perspective in a timely manner is to have a task created for a responsible IT security entity to independently verify the security requirements during the commissioning process. This method has several significant implications for the business processes and operations. For instance, this would potentially slow down the commissioning process. A lot more resources are required to attend the large number of newly commissioned network devices. Plus, there are costs associated with the manpower required to work overtime as many of the commissioning changes take place after business hours, on weekends, and holidays to avoid service interruption.

As a matter of fact, in organizations with a large number of network devices, identifying security weaknesses is not a big challenge; where security assessment tools can be used to perform the security verification on a regular basis or on-demand. However, security assessment tools by themselves would not be capable of addressing the timely verification out of the box as that requires some kind of intelligence and customization to be efficiently functioning within the enterprise-specific IT environment.

II. EFFICIENT APPROACH FOR TIMELY SECURITY ASSESSMENT

We need to make sure before considering any approach and putting it into practice, it should not only meet our requirement by addressing the timely security assessment, but also avoids all the constraints and implications posed by the traditional way as highlighted earlier. My approach that will be discussed in this paper is a combination of a process, technology, and some sort of software development to develop the required intelligence.



Process

A robust process is required to for this approach to work efficiently. Segregation of duty is one of the cornerstone elements of this process. When deploying a new device, there should be at least two independent entities handling this task:

- Operations taking care of the commissioning
- Security responsible for the assessment

It is mandatory for IT operations to properly document the newly added device through either an asset inventory or monitoring system as part of the commissioning process. This includes device IP addresses, types of the device, the entity that will be managing the device, and so on.

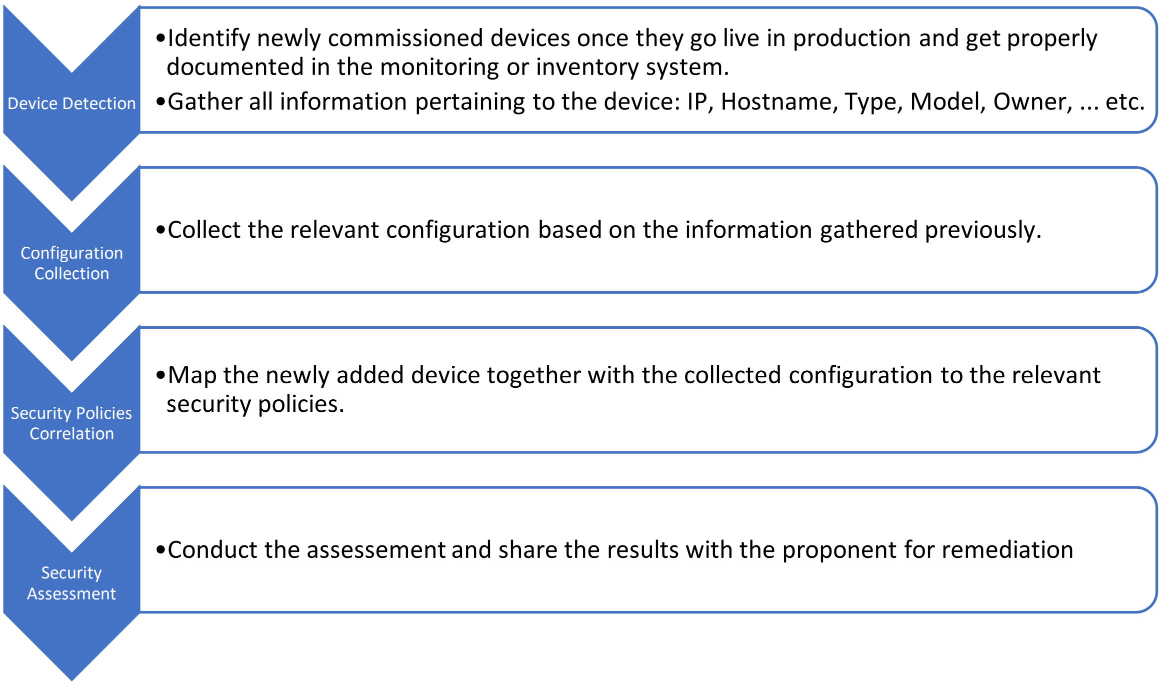
Technology

As highlighted earlier, commercial security assessment tools are commonly used by organizations although some organizations might develop their own tools that fulfil their basic requirements. These tools are used to conduct regular scanning activities looking for vulnerabilities or security misconfigurations. It is imperative that these tools, developed either commercially or in-house, support an application programming interface (API) to be able to define the interactions between the security tools and the intelligence that will be developed to achieve the real-time security assessment for network devices and appliances.

Software Development

This is the most crucial part of this approach as it requires substantial effort for coding and customization to ensure the synchronization with the security assessment tools and they both work hand in hand. That being said, I will focus more on the concept in this section as this can be implemented differently using different programming languages.

This software that needs to be developed, should contain a set of APIs that call the appropriate functions from both asset inventory and security assessment tools to perform the following tasks:


Device Detection
•Identify newly commissioned devices once they go live in production and get properly documented in the monitoring or inventory system.
•Gather all information pertaining to the device: IP, Hostname, Type, Model, Owner, ... etc.
Configuration Collection
•Collect the relevant configuration based on the information gathered previously.
Security Policies Correlation
•Map the newly added device together with the collected configuration to the relevant security policies.
Security Assessment
•Conduct the assessement and share the results with the proponent for remediation

It should be seamlessly triggered once a new device goes live in production and gets properly added and documented in the monitoring system or asset inventory. So, if a new device gets commissioned, this software should be capable to perform the following actions:

- Information Gathering and Asset Identification: Identify the newly added device, collect all related information to be utilized for security verification.

- Inform the concerned entity once new network device commissioning occurs: Notification of a new commissioning in a form of email is sent to the appropriate entity just in case if further requirements need to be addressed by the security analysts.

- Add newly commissioned device to the security tool for continuous monitoring: the collected device information is encapsulated be fed to the security assessment tool and mapped to the relevant security policies for assessment.

- Assess the security of the device once added: Conduct security assessment once the device is added.

- Send a report of findings to the proponent once assessed: The results of the assessment are shared with the proponent to act accordingly. The device can either continue its way to production or suspended from being connected to the network.

Identifying decommissioned devices should be part of the intelligence of the software as well. Monitoring and assessing decommissioned devices, using the security tools, is considered waste of resources including but not limited to network bandwidth, man-hours for maintenance, and money (each IP address is tied with a license that costs money). Therefore, timely alert and action of decommissioned systems is key to get these systems removed from the security tools to maintain efficient utilization of resources. Therefore, the below set of actions of the decommissioning will be triggered once an existing device gets removed from the proponent monitoring system/asset inventory:

- Information Gathering and Asset Identification: Identify the device that has been decommissioned.

- Inform the concerned entity once decommissioning occurs: A notification in a form of email is sent to the appropriate entity just in case there are additional requirements need to be addressed by the security analysts.

- Remove decommissioned devices from the security configuration assessment tool: The records for the decommissioned devices are removed from the security tool to stop monitoring them.

III. CONCLUSION

Timely security assessment against newly deployed systems is imperative to maintain the security and protection of the enterprise assets. This can be technically achieved for systems that can host security agents such as Windows and Linux. Systems such as network devices and appliances would pose a significant cybersecurity risk if not assessed once deployed to the network. To properly and efficiently address the risk, organizations should consider a mechanism that might require either establishment of a new process, technology, and software development or some improvements on them if these are already existing.

It is very important that new devices are properly documented in an asset inventory before they are commissioned. It is also essential that the security tools used to perform a regular security assessment do support APIs as these need to be called by the software that would provide the required capability to immediately assess newly added devices.

The software should be designed and developed to automatically detect network devices commissioned in real time. It should be able to conduct a security assessment right after they get activated and commissioned in the IT infrastructure. Newly detected devices are automatically mapped to the relevant security policies and assessments. The solution alerts security analysts as well as network administrators for any deviations and security weaknesses.

In case a network device is decommissioned or removed from the IT infrastructure, the solution will detect the removal. It will remove this device from all future assessments and scans. This helps in conservation of licenses and helps in optimization of cost.