Challenge #2

By

Stalin Peña

7/6/16

Executive Summary

Skyfall, an infrastructure and security company has been tasked by our Billionaire friend to supervise the security of the internal and external components of the datacenters located on Earth and the moon including their channels of communication. Before Skyfall takes over the security of the datacenters, it has been communicated of the suspiciousness that the communication between the datacenters on Earth and the moon has been compromised by an unknown third party.

The suspicion that the satellite communication between the datacenters on Earth and the Moon has been compromised was confirmed after alterations were found on the last shipping manifest of goods that were supposed to be shipped to the datacenter on Earth by a goods distribution company located in the State of New Mexico. The internal security team has not been able to identify the culprit until now.

Skyfall has started to develop a plan of action in order for them to be able to identify how the security and the communication between the datacenters was compromised in the first place, who is responsible for compromising the satellite link between both datacenters and for how long this breach in security has been happening.

Project Requirements

PRQ1	Find the extent of the changes anywhere within the system. What are the prereqs to make this happen?
PRQ2	Be notified of other changes. Not just to files but to attacks. What are the steps of an attack? How fast can you detect an attack and changes?
PRQ3	Prevent changes. Can you just detect the attack or prevent the attacked?
PRQ4	Determine the root of the attack. Can we find the culprit? Is there any forensics data? Where did the bad actor leave his or hers fingerprints? Is the black market or something else?

Project Risks

PR1	Data satellite link has been compromised and it also under the control of the bad actor or

	organization.
PR2	Internal network might also be monitored by the bad actor.
PR3	Internal Role based authentication system might be compromised as well.
PR4	Vendor Order placing system is unknown
PR5	Tipping off the bad actor or organization

Project Constraints

PC1	The amount of system data that have been compromised is unknown.
PC2	For how long the data has been compromised is unknown.
PC3	Access to a secondary Satellite for data transmission between Earth and the Moon datacenter is unknown.

Project Assumptions

PA1	Old shipping manifest are available
PA2	Budget for Double authentication system will be approved immediately
PA3	Double authentication systems implemented at datacenter level will also be implemented at the datalink level between Earth and the moon.
PA4	Servers and security devices have been configured to log data into syslog servers.

Skyfall's Security design Proposition

After meetings with the datacenter management and security teams, Skyfall is recommending a plan of attack which will allow them to prevent security exploits, detect attacks to internal and external components of the datacenters and their satellite communication links.

At the Internal components of the datacenter, Skyfall recommends the following:

At the server level

1- Create gold images of each server type.

2- Setup production servers to be read only servers which will boot from its corresponding gold image.
3- Make the network where the servers are booting from non-routable to prevent external attacks.
4- Servers gold images will only be updated and patched by Skyfall's senior staffers on a parallel internal infrastructure independent of the datacenter production servers.
5- Hypervisor servers will be configured to send their logs to a centralized cluster of syslog server which will be installed at each datacenter.

At the Network level

1- All the Physical Firewalls internal to the datacenters will be recommended to be replaced. A Double firewall hop will be utilized to prevent external unauthorized traffic from reaching the internal servers located at each datacenter.
2- Physical Firewall's configuration will be encrypted with 10K bytes encryption and changes to any configuration will need to be approved by an official party of Skyfall security engineers. Without obtaining approval of each member, configuration changes will not be applied and will generate and immediate security alarm.
3- The virtual server communication will be segmented utilizing software defined firewalls which will push firewall rules based on policies that have been composed by Skyfall's security team.
4- Network ports at every physical switch will be setup to be in administrative shutdown mode to be prevent traffic that has not be configured by the Network and security team.

At the storage Level

1- Skyfall has developed a software suite which reports when modifications have been performed at each file stored in each Storage Area Network located at each datacenter. This software suite will report the username, time and physical location of the user when any file is modified. The audit information generated by the software suite will be stored inside a database cluster which will be installed at each datacenter.
2- The information stored at the database cluster will be scanned every 30 minutes by the software suite audit technology looking permission modifications and file modifications that have not been approved.

Role based Authentication and Authorization System

A new Role based authentication system will be implemented which will prompt every user to authenticate using a two factor authentication with the network directory services using a 3 level security system. The first levels of authentication will be:

a- Iris Scanner
b- Fingerprint Scanner
c- Voice Scanner

The second level of security or authorization will be implemented by injecting a security chip in each employee's forearm which will be required to complete the two form factor authentication system.

Communication system

It has been expressed to Skyfall that the most pressing issue to resolve is to take over the control of the satellite communication between both datacenters. To resolve this situation Skyfall is recommending the use of a two steps process:

1- Setup a secondary Satellite link for datacenter communications. The secondary satellite link will be connected to a separate satellite that is orbiting Earth and positioned half way from the first satellite.
2- The management of the second satellite connection will be performed by Skyfall and any configuration changes will be performed using the same two factor authentication method but, the directory services will be different than the datacenter network.
3- To take back management control of the first satellite communication link Skyfall is recommending failing communications to the secondary communications link and then resetting the management controls of the first link to factory default. Once the settings are back to factory defaults, the management controls will be setup to use the new proposed authentication methods.
4- Both satellite link communications will be encrypted with state of the art 100K bytes cypher algorithm.

Purchasing System

In order to prevent the purchasing system to be compromised as again, Skyfall will request the distribution company for old shipping manifest for investigation. The investigation will look for route and product deviations. In the meantime, all new orders will need to be placed using a brand new purchasing system develop by Skyfall that monitors the locations of every company truck by satellite (Satellite own and operated by Skyfall). Shipments need to be reviewed and approved by the datacenter internal security team and Skyfall. If deviations are found during route, the trucks will be automatically rerouted back to base immediately. The new system will continue to scan the shipment manifest for modifications every 5 minutes.