**OSPenTek Solutions - Security Operation: Preventive Actions**

**Company Mission**

OSPenTek Solutions is dedicated to protecting IT infrastructures through cutting-edge solutions and high-level consulting, aiming to identify and mitigate risks to prevent security breaches that could compromise operations and clients' sensitive information.

**Detailed Quote**

**Immagine che contiene testo, schermata, numero, Carattere

Descrizione generata automaticamente**

**Report S9\_L1**

**Exercise Objective:**

As an external consultant for OSPenTek Solutions, my goal was to verify the impact of activating the Firewall on a Windows XP machine on the results of an external service scan. I used Nmap for this evaluation, trying to identify how Firewall changes affect the visibility of services offered by the machine.Immagine che contiene testo, schermata, Carattere, documento

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, algebra

Descrizione generata automaticamente

**Machine Setup:**

* **Virtual Machines:** For this exercise, two virtual machines were set up in an isolated environment. One ran Kali Linux, used for security scans, while the other was based on Windows XP and served as the target.
* **Network Configuration:** Both machines were connected in "Bridged Adapter" mode, allowing network interactions as in a production environment

Immagine che contiene testo, schermata, Carattere, grafica

Descrizione generata automaticamente

**IP Address Configuration:**

* **Windows XP:**Configured with a static IP address of 192.168.240.150 and a subnet mask of 255.255.255.0.

Immagine che contiene testo, elettronica, schermata, software

Descrizione generata automaticamente

* **Kali Linux:**Configured with a static IP address of 192.168.240.100 and a subnet mask of 255.255.255.0, set through modifications to the network configuration file.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**Test Scenarios:**

**1. First Scenario - Firewall Disabled:**

* Deactivation of the Firewall on Windows XP via Control Panel.
* Execution of an Nmap scan from Kali Linux to Windows XP: nmap -sV -oA scan\_result1 192.168.240.150.
* Results: Detection of numerous open services, with extensive details on protocols and operating systems.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**Second Scenario - Firewall Enabled:**

* Activation of the Firewall on Windows XP.
* New Nmap scan executed: nmap -sV -oA scan\_result2 192.168.240.150.
* Results: Substantial differences compared to the first scenario, with the machine appearing offline, indicating that all external requests were effectively blocked.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**Analysis of Differences:**

The differences noted between the results of the two scans are significant. In the first scenario, with the Firewall disabled, Nmap managed to detect open services and provide detailed information about the Windows XP machine, such as the operating system and protocols used. In contrast, in the second scenario, with the Firewall enabled, Nmap was unable to obtain the same details and indicated that the host appeared offline.  
The cause of this different result is the activation of the Firewall on the Windows XP machine. When the Firewall is active, it acts as a security barrier, filtering incoming traffic and blocking ping requests from Nmap. Consequently, Nmap cannot establish a direct connection with the target machine and cannot collect detailed information about services and the operating system.

**Conclusions:**

The analysis conducted demonstrates that activating the Firewall on a Windows XP machine has a considerable impact on the results of external security scans. The Firewall serves as an important preventive measure, not only hiding details of open services but also making the host completely unreachable from external scans. This underscores the importance of the Firewall as an essential component in protecting computer systems against attacks.