CLIENTE:\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

FECHA: miércoles 21-02-2024 V1 \_

HORA DE LLEGADA:\_\_ 03:45 pm \_\_\_\_\_

HORA DE SALIDA: \_\_ 07:51 pm \_\_\_\_

ARMANDO LOPEZ

Tlf: 04142871877

04241996098

Trabajos realizados Armando López

INTERNET: SERVIDORES: CORREOS: SOPORTE PC: SOPORTE USUARIOS: REDES: VARIOS:

SEGURIDAD: APLICACIONES:

SERVIDORES:

\* VMC2DC: - Se enlazó GPO Windows Firewall log creation al dominio DMNCAC.COMARCA.COM.VE. Se usó simulación de uso de gpo con GROUP POLICY MODELING WIZARD con usuario dmncac\admincomarca y computadora VM3FM. – Creación de nueva gpo y enlace al dominio con permisos para AUTHENTICATED USERS:

**SET POWERSHELL EXECUTION POLICY TO REMOTE SIGNED🡪Computer Configuration🡪 Policies🡪 Administrative Templates🡪 Windows Components🡪 Windows Powershell🡪Turn on script execution=ALLOW LOCAL SCRIPTS AND REMOTE SIGNED SCRIPTS.**

– Creación de nueva gpo y enlace al dominio con permisos para AUTHENTICATED USERS:

**Copy script for FIREWALL changes to PREVENT RDP BRUTE FORCE ATTACKS🡪 Computer Configuration🡪 Preferences🡪Windows Files🡪ACTION=UPDATE,**

**source file=[\\vmc2dc\NETLOGON\scripts\RDC\_Brute\_Force\_Prevention.ps1](file:///\\\\vmc2dc\\NETLOGON\\scripts\\RDC_Brute_Force_Prevention.ps1) ,**

**destination file= c:\scripts\RDC\_Brute\_Force\_Prevention.ps1**

– Creación de nueva gpo y enlace al dominio pero de nuevo restringiendo el SCOPE🡪SECURITY filtering a DOMAIN USERS (USUARIOS) Y VM3FM$, VM5$ y HaiderALtestW10$ (computadores) para que la política aplicara solamente a pruebas de 3 computadoras con: Window Server 2008 (VM3FM,VM5) y Windows 10 (HaiderALtestW10). También para prevenir efectos de aplicación futura a configuraciones manuales en vez de con GPO se cambió la configuración avanzada de la GPO para excluir servidores VM1SQL, VM4RUBY Y SERVERHPG6: GPMC🡪GROUP POLICY OBJECTS🡪 **Block Brute Force RDP Attacks SCHEDULED TASK🡪DELEGATION🡪ADVANCED🡪Se agregó servidores VM1SQL, VM4RUBY Y SERVERHPG6🡪FULL CONTROL=DENY (para evitar evitar permisos READ=ALLOW y APPLY GROUP POLICY=ALLOW).**

**Block Brute Force RDP Attacks SCHEDULED TASK🡪 Computer Configuration🡪 Preferences🡪 CONTROL PANEL SETTINGS🡪SCHEDULED TASKS🡪NEW SCHEDULE TASK (AT LEAST WINDOWS 7)🡪GENERAL: USER=SYSTEM, run with highest privileges, Run whether user is logged on or not, TRIGGERS: the task starts the day it is implemented, at 12:00 pm, recurs every 1 day, every 5 minutes, and stops after 30 minutes, ACTIONS: Start a program🡪**

**Program/script = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe**

**ARGUMENTS= -file c:\scripts\RDC\_Brute\_Force\_Prevention.ps1**

\* VM3FM, VM5 y HaiderALtestW10: - ejecución de GPUPDATE /FORCE y se creó en Windows de log de firewall de Windows con gpo.

\* Revisión de configuraciones de “powershell execution policies” para habilitar política para ejecución local de scripts de powershell en Windows Clients y Windows Servers. Se tuvo que reiniciar Windows para aplicar la configuración de COMPUTER CONFIGURATION de la GPO y se realizaron los cambios deseados con la política “**SET POWERSHELL EXECUTION POLICY TO REMOTE SIGNED”** cuya aplicación se verificó en powershell con get-execution policy=remoteSigned. – Se repitió ejecución de **GPUPDATE /FORCE** y se logró copiar archivo a **c:\scripts\RDC\_Brute\_Force\_Prevention.ps1** ejecutando gpo “**Copy script for FIREWALL changes to PREVENT RDP BRUTE FORCE ATTACKS**” . Se enlazó también al dominio gpo **Block Brute Force RDP Attacks SCHEDULED TASK** y funcionó parcialmente creando SCHEDULED TASK pero falló la creación de la nueva regla de bloqueo en FIREWALL DE WINDOWS. Se continuará arreglos posteriormente.

Cliente (recibido): Armando López

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Observaciones:

4 horas 00 minutos facturables ( va(n) 4 hora(s) 0 minutos)

0 horas **NO** facturables:

**SOPORTE REMOTO**

.