sedian

Seguridad Digital
de Andalucía

Charla virtual

Ataques a escritorios remotos en tiempos de coronavirus y cómo protegernos

Julio 2020

Junta de Andalucía

SOBRE MÍ

Jesús D. Angosto Iglesias

Cybersecurity Auditor & Forensics Analyst

Ingenia

linkedin.com/in/jdangosto

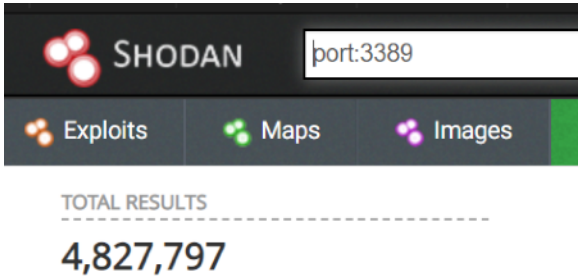
@jdangosto

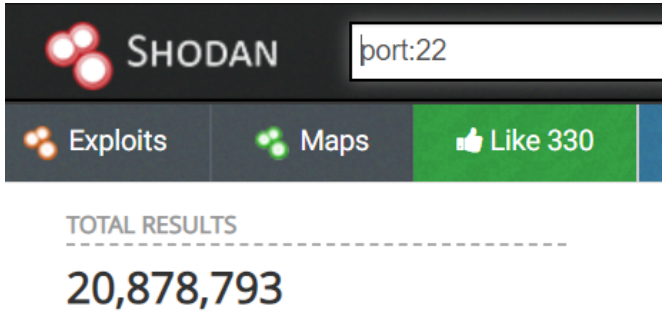
OBJETIVOS

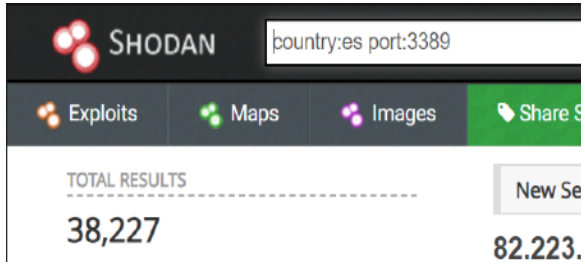
- Conocer el funcionamiento del RDP
- Qué logs deja en el sistema un escritorio remoto
- Reproducción de ataques, con el objetivo de ver su sencillez
- Qué rastro puede dejar un ataque al escritorio remoto
- Cómo podemos mitigar dichos ataques

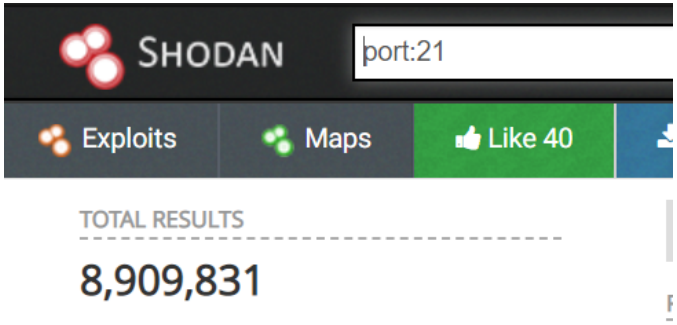
Teletrabajo

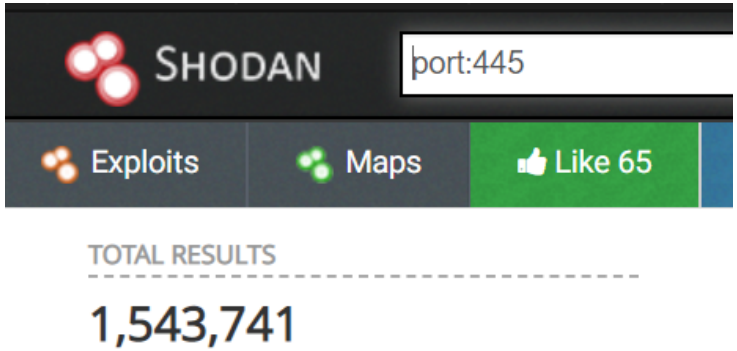
sedian Seguridad Digital de Andalucía


SHODAN
port:3389
Exploits
Maps
Images
TOTAL RESULTS
4,827,797


SHODAN
port:22
Exploits
Maps
Like 330
TOTAL RESULTS
20,878,793


SHODAN
country:es port:3389
Exploits
Maps
Images
TOTAL RESULTS
38,227
New Se
82.223.


SHODAN
port:21
Exploits
Maps
Like 40
TOTAL RESULTS
8,909,831


SHODAN
port:445
Exploits
Maps
Like 65
TOTAL RESULTS
1,543,741

Incremento de ciberataques por el Covid

sedian Seguridad Digital de Andalucía

https://www.ccn-cert.cni.es/cibercovid19/informes-covid19.html

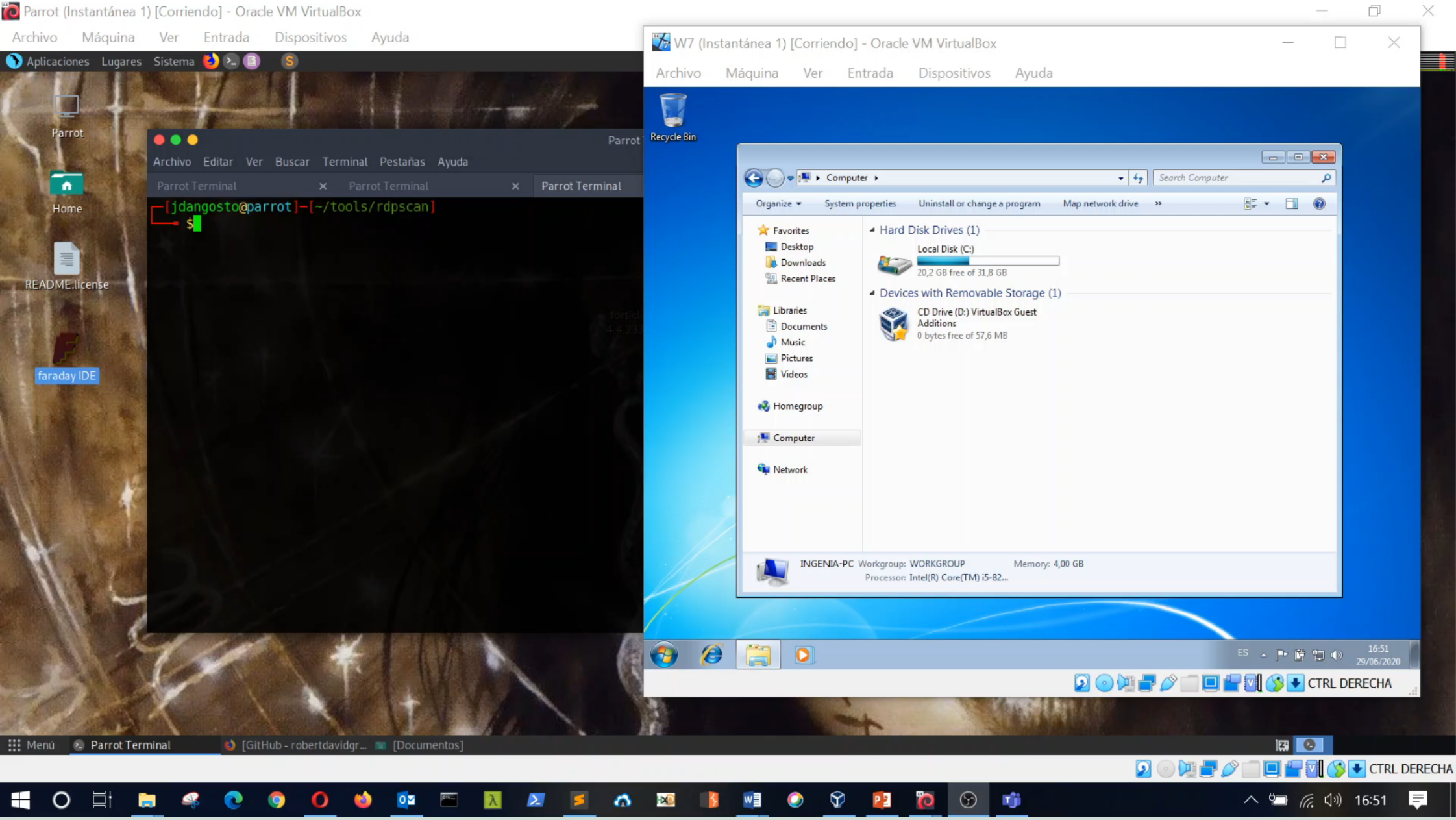
Demo time!

Vulnerabilidad en Windows RDP

BlueKeep

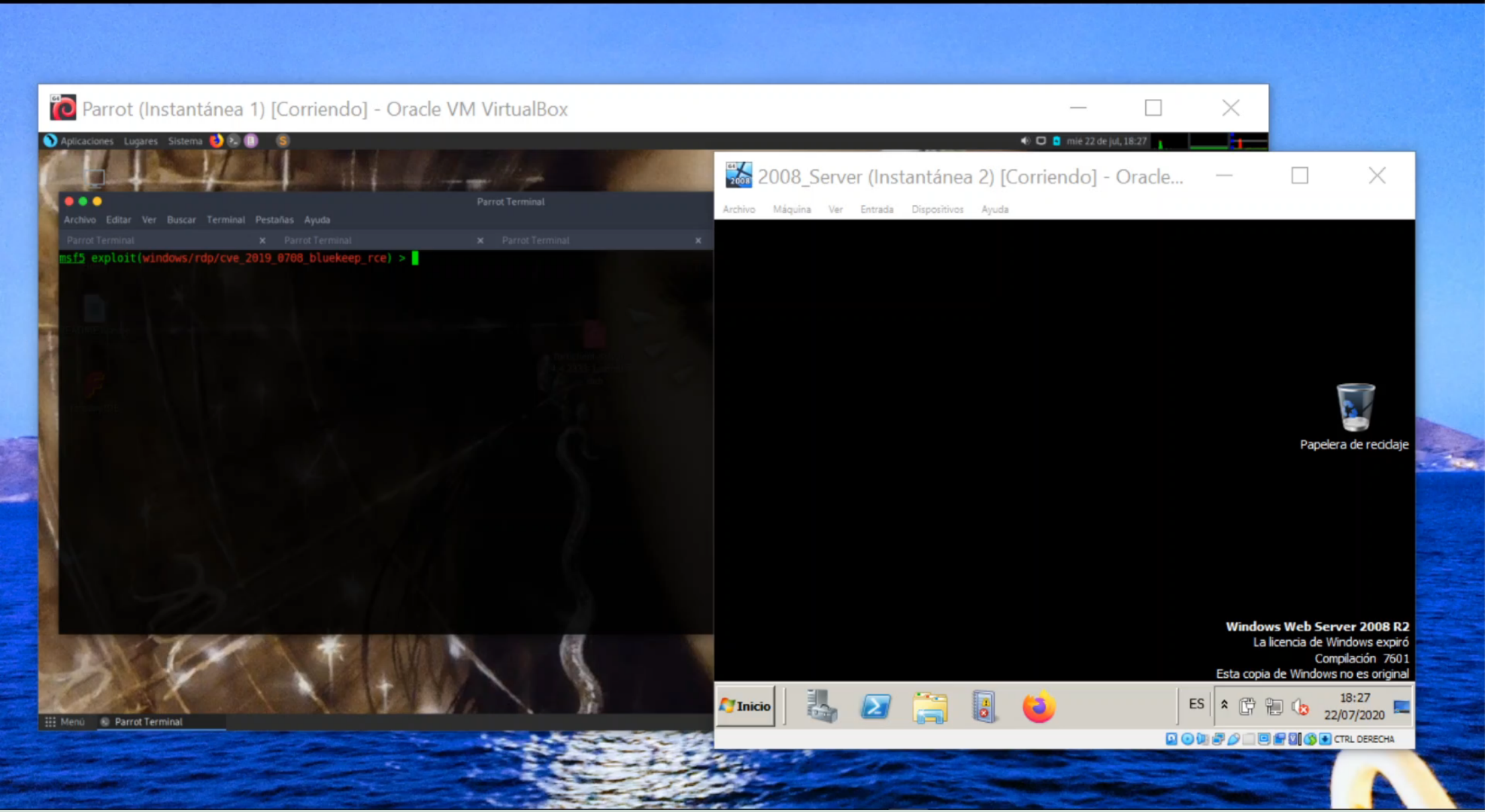
BlueKeep — CVE-2019–0708

sedian Seguridad Digital de Andalucía



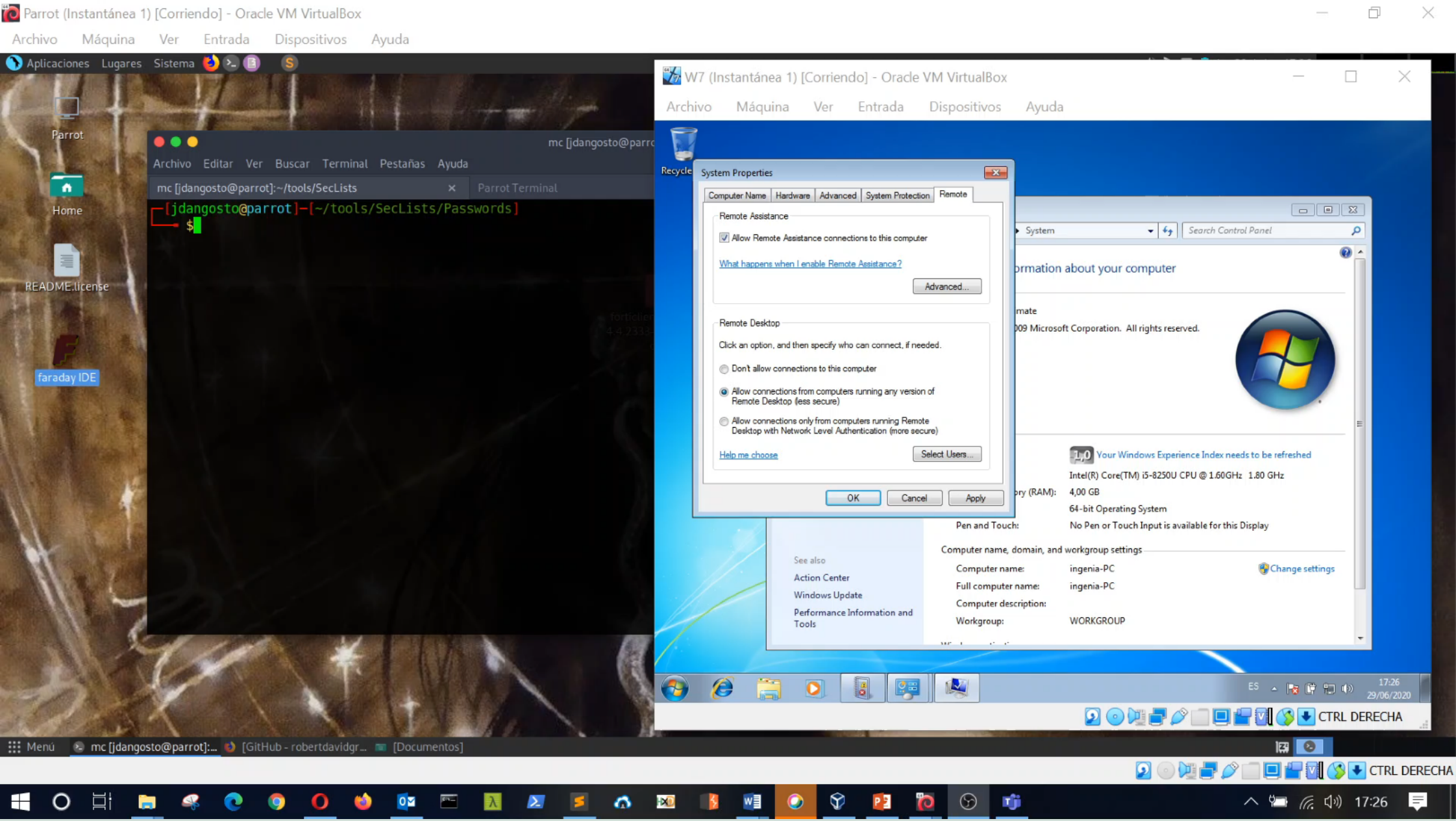
sedian Seguridad Digital de Andalucía

Demo:
BlueKeep – Denegación de servicio
Windows 2008 Server R2



sedian Seguridad Digital de Andalucía

Demo:
MITIGACIÓN DE EXPLOTACIÓN RDP



sedian Seguridad Digital de Andalucía

Parches publicados: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability

Security Vulnerability

Published: 05/14/2019
MITRE CVE-2019-0708

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

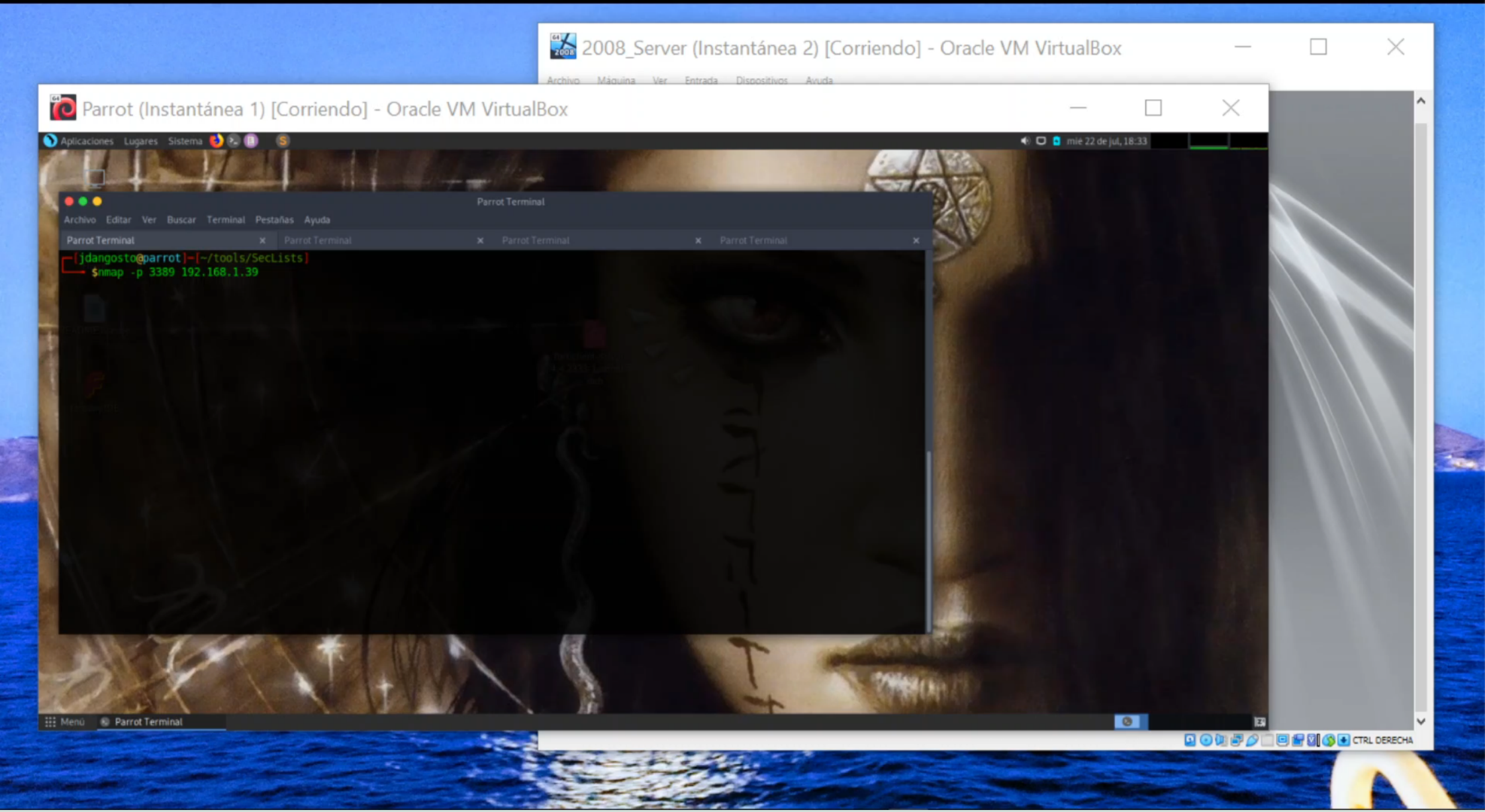
The update addresses the vulnerability by correcting how Remote Desktop Services handles connection requests.

BRUTE FORCE ATTACK

sedian Seguridad Digital de Andalucía

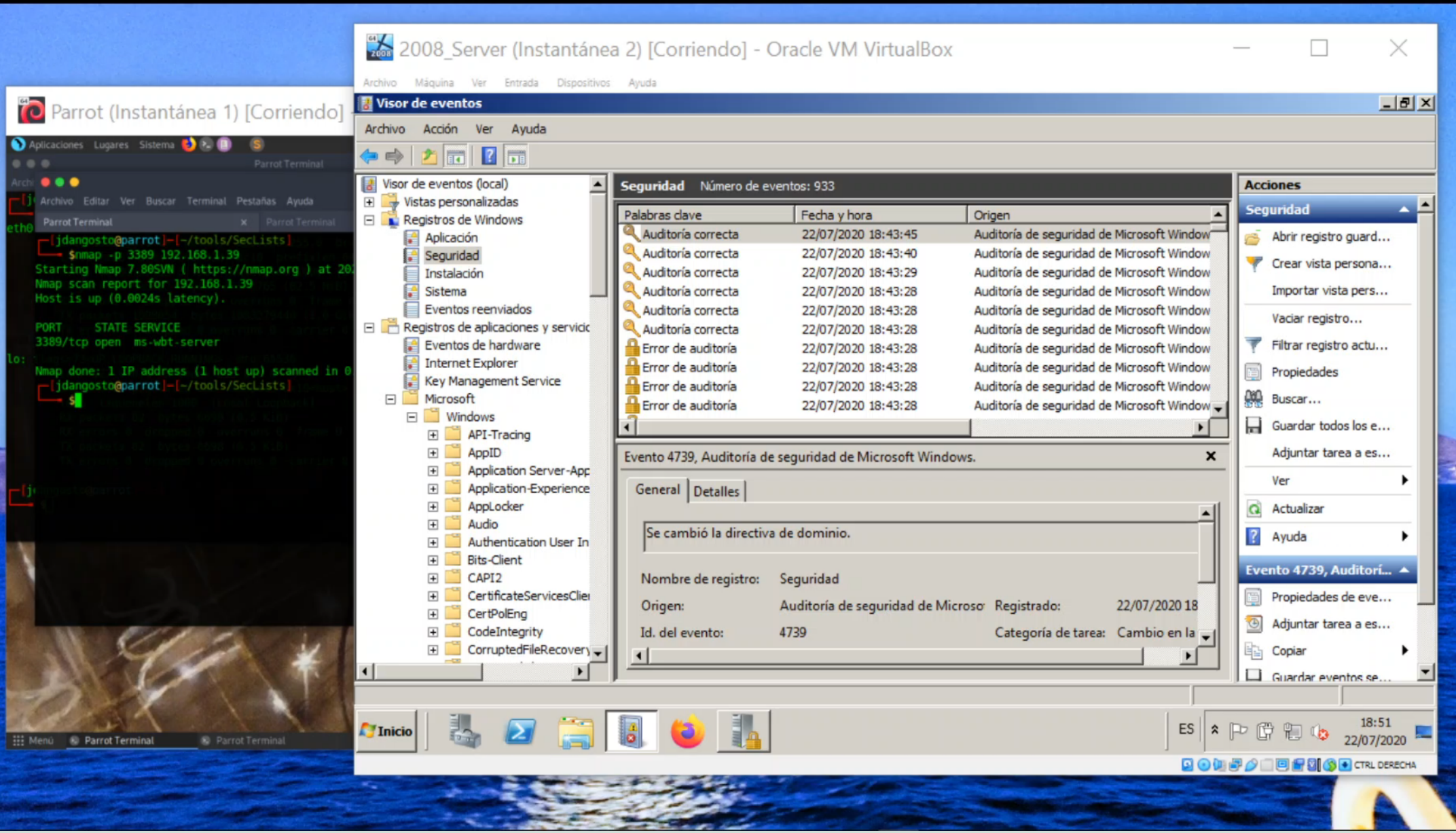
THC- Hydra

Herramienta Open Source para ataques de fuerza bruta



sedian Seguridad Digital de Andalucía

¿Qué genera un ataque por fuerza bruta en el sistema?

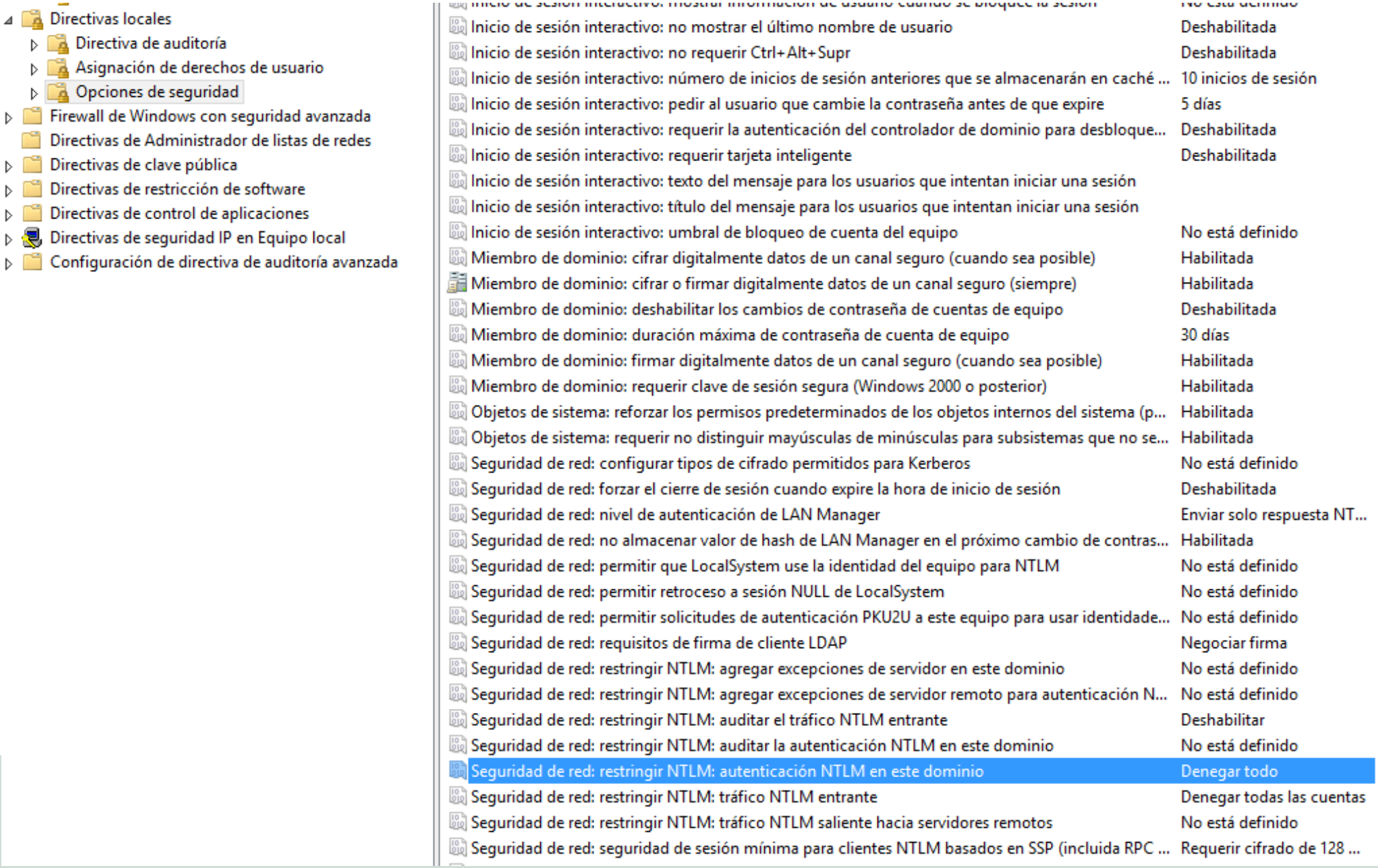


sedian Seguridad Digital de Andalucía

¿Es posible bloquear un ataque por fuerza bruta en el sistema?

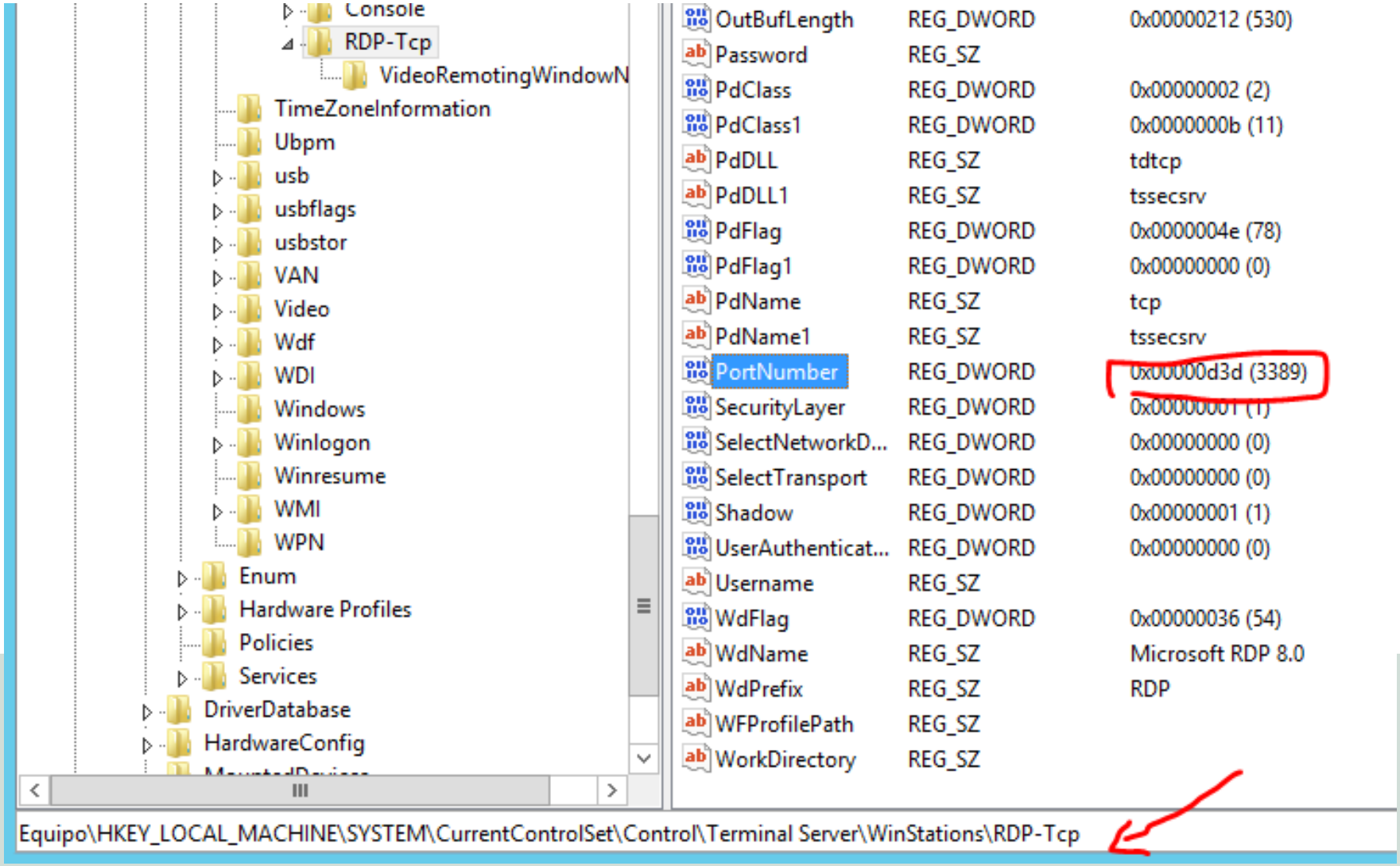
SOLUCIONES:

- Restringir conexiones y tráfico basado en autenticación NTML.
- Política de contraseñas y bloqueo de cuentas
- Grupo para conexiones RDP
- Bloqueo de IP atacante a nivel de Firewall
- Cambiar puerto RDP (Opcional)

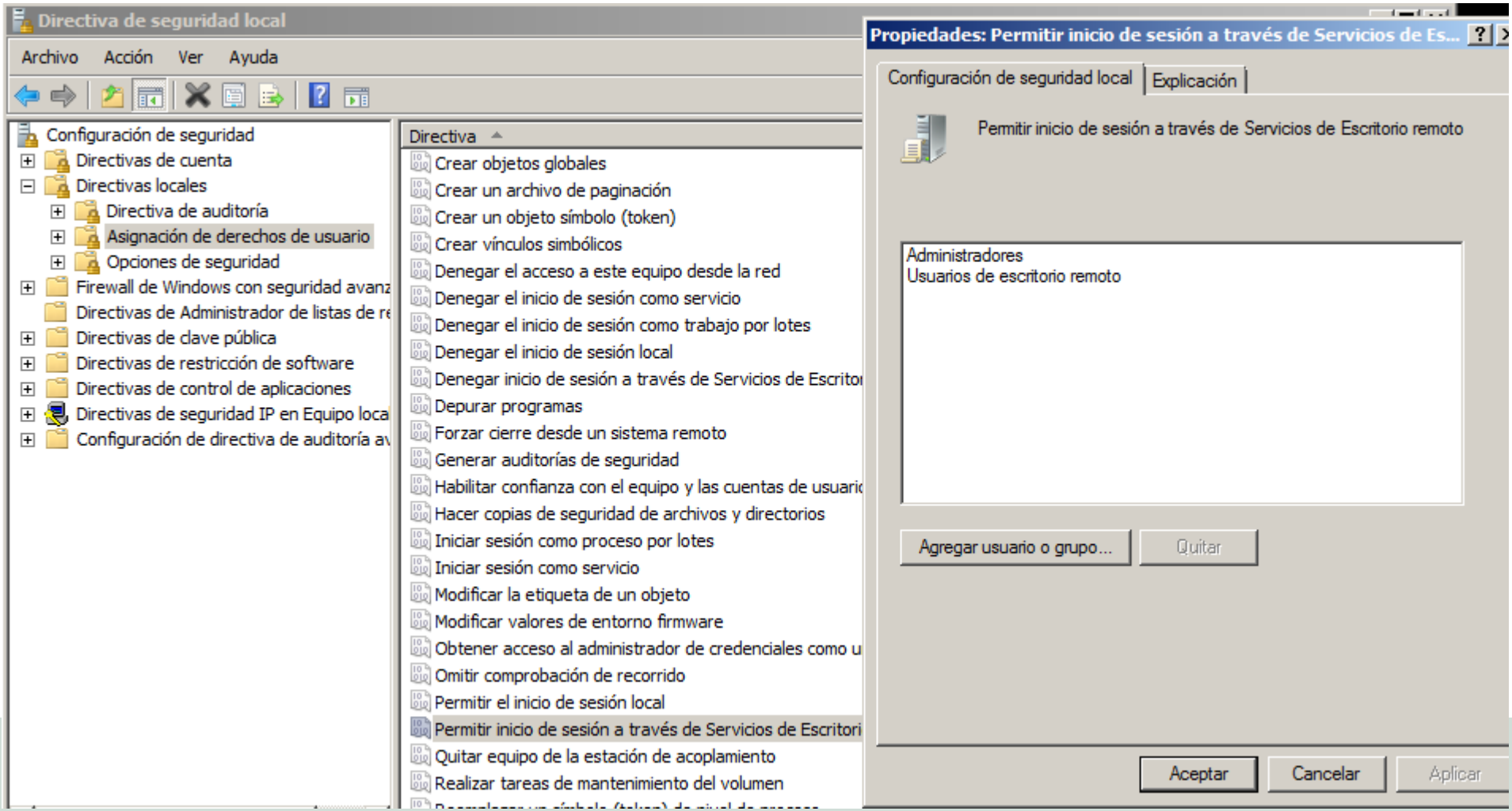

Directivas locales
Directiva de auditoría
Asignación de derechos de usuario
Opciones de seguridad
Firewall de Windows con seguridad avanzada
Directivas de Administrador de listas de redes
Directivas de clave pública
Directivas de restricción de software
Directivas de control de aplicaciones
Directivas de seguridad IP en Equipo local
Configuración de directiva de auditoría avanzada
Inicio de sesión interactivo: no mostrar el último nombre de usuario Deshabilitada
Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr Deshabilitada
Inicio de sesión interactivo: número de inicios de sesión anteriores que se almacenarán en caché ... 10 inicios de sesión
Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire 5 días
Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloque... Deshabilitada
Inicio de sesión interactivo: requerir tarjeta inteligente Deshabilitada
Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión
Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión
Inicio de sesión interactivo: umbral de bloqueo de cuenta del equipo No está definido
Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible) Habilitada
Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre) Habilitada
Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo Deshabilitada
Miembro de dominio: duración máxima de contraseña de cuenta de equipo 30 días
Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible) Habilitada
Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior) Habilitada
Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (p... Habilitada
Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no se... Habilitada
Seguridad de red: configurar tipos de cifrado permitidos para Kerberos No está definido
Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión Deshabilitada
Seguridad de red: nivel de autenticación de LAN Manager Enviar solo respuesta NT...
Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contras... Habilitada
Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM No está definido
Seguridad de red: permitir retroceso a sesión NULL de LocalSystem No está definido
Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidade... No está definido
Seguridad de red: requisitos de firma de cliente LDAP Negociar firma
Seguridad de red: restringir NTLM: agregar excepciones de servidor en este dominio No está definido
Seguridad de red: restringir NTLM: agregar excepciones de servidor remoto para autenticación N... No está definido
Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante Deshabilitar
Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio No está definido
Seguridad de red: restringir NTLM: autenticación NTLM en este dominio Denegar todo
Seguridad de red: restringir NTLM: tráfico NTLM entrante Denegar todas las cuentas
Seguridad de red: restringir NTLM: tráfico NTLM saliente hacia servidores remotos No está definido
Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC ... Requerir cifrado de 128 ...

CAMBIAR PUERTO RDP

HKLM\SYSTEM\CurrentControlSet\TerminalServer\WinStations\RDP-TCP >> PortNumber

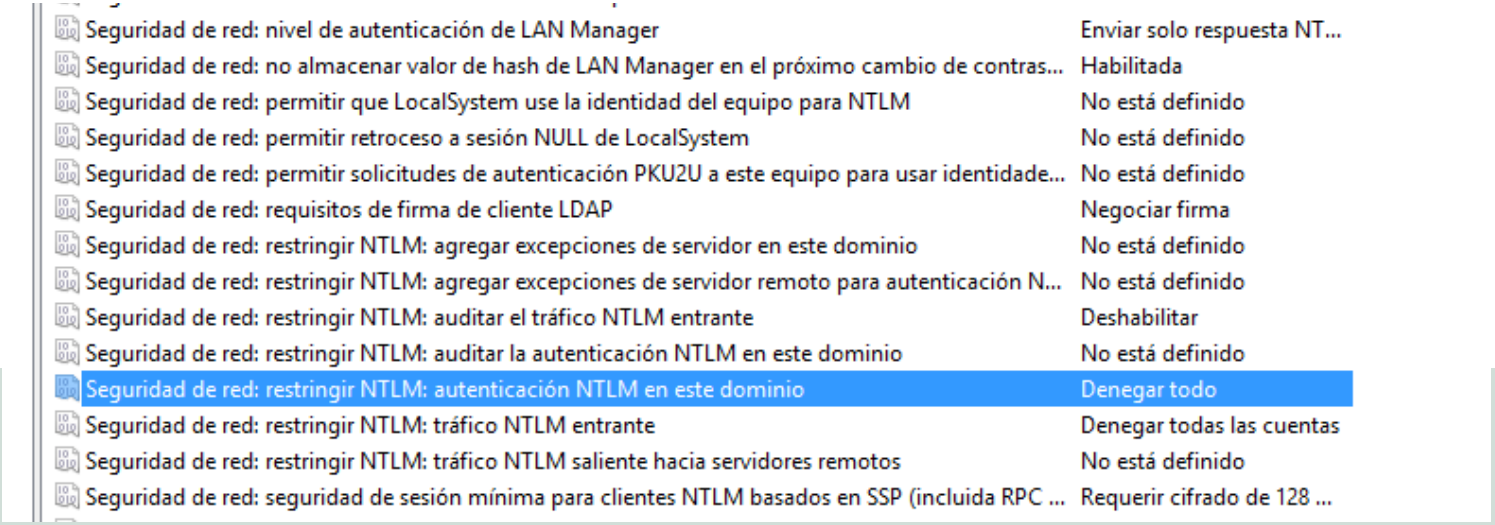


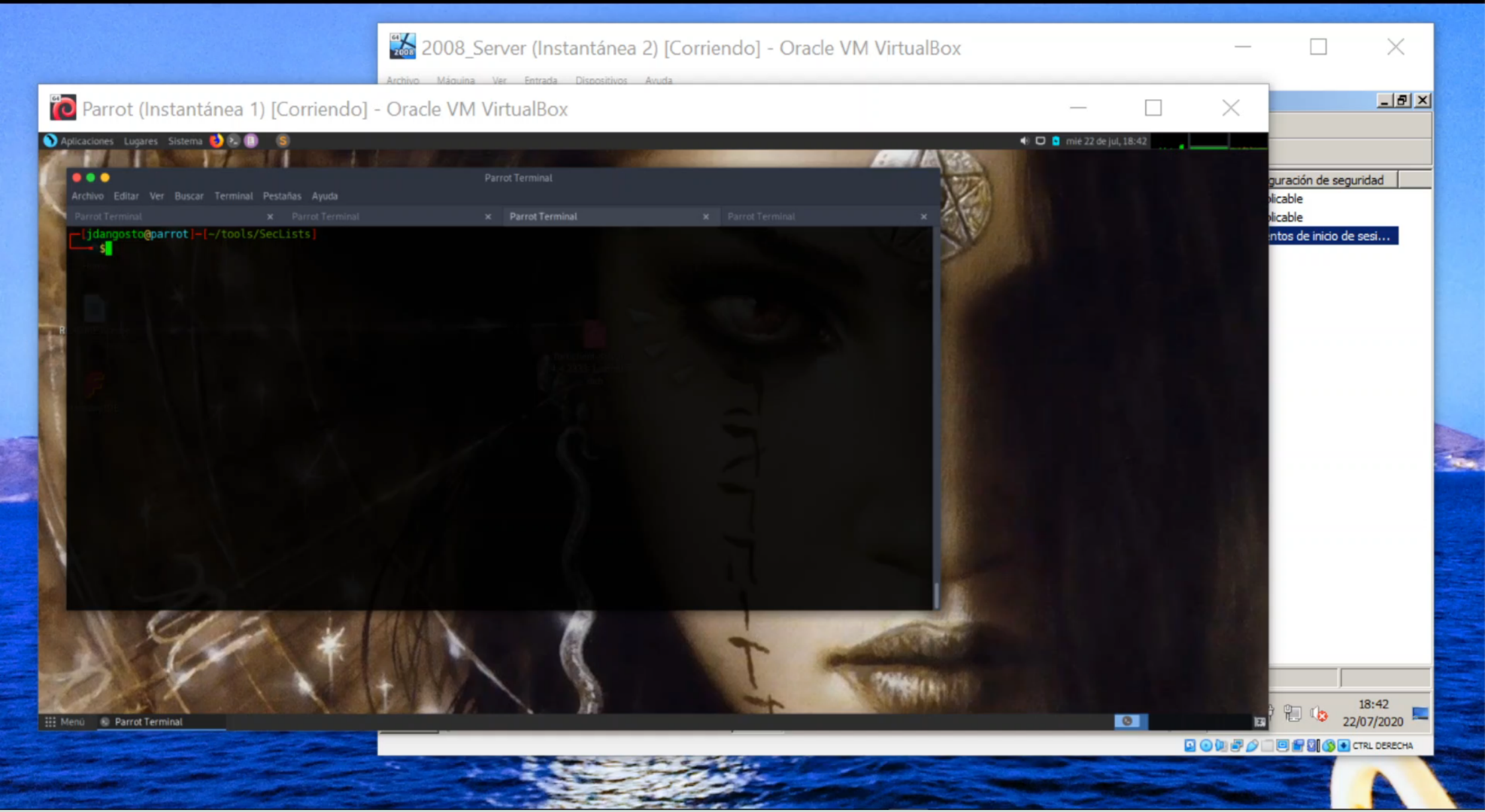
Directiva Inicio de sesión para Escritorios Remotos



RESTRICCIÓN NTLM

- Inicio > Ejecutar > secpol.msc
- Directivas Locales > Opciones de Seguridad
- Seguridad de red: nivel de autenticación de LAN manager
- (Enviar sólo respuesta NTLMv2 y rechazar LM y NTLM)
- Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante (Habilitar)
- Seguridad de red: autenticación NTLM en este dominio (Denegar todo)
- Seguridad de red: restringir NTLM: autenticación NTLM en este dominio (Denegar todo)

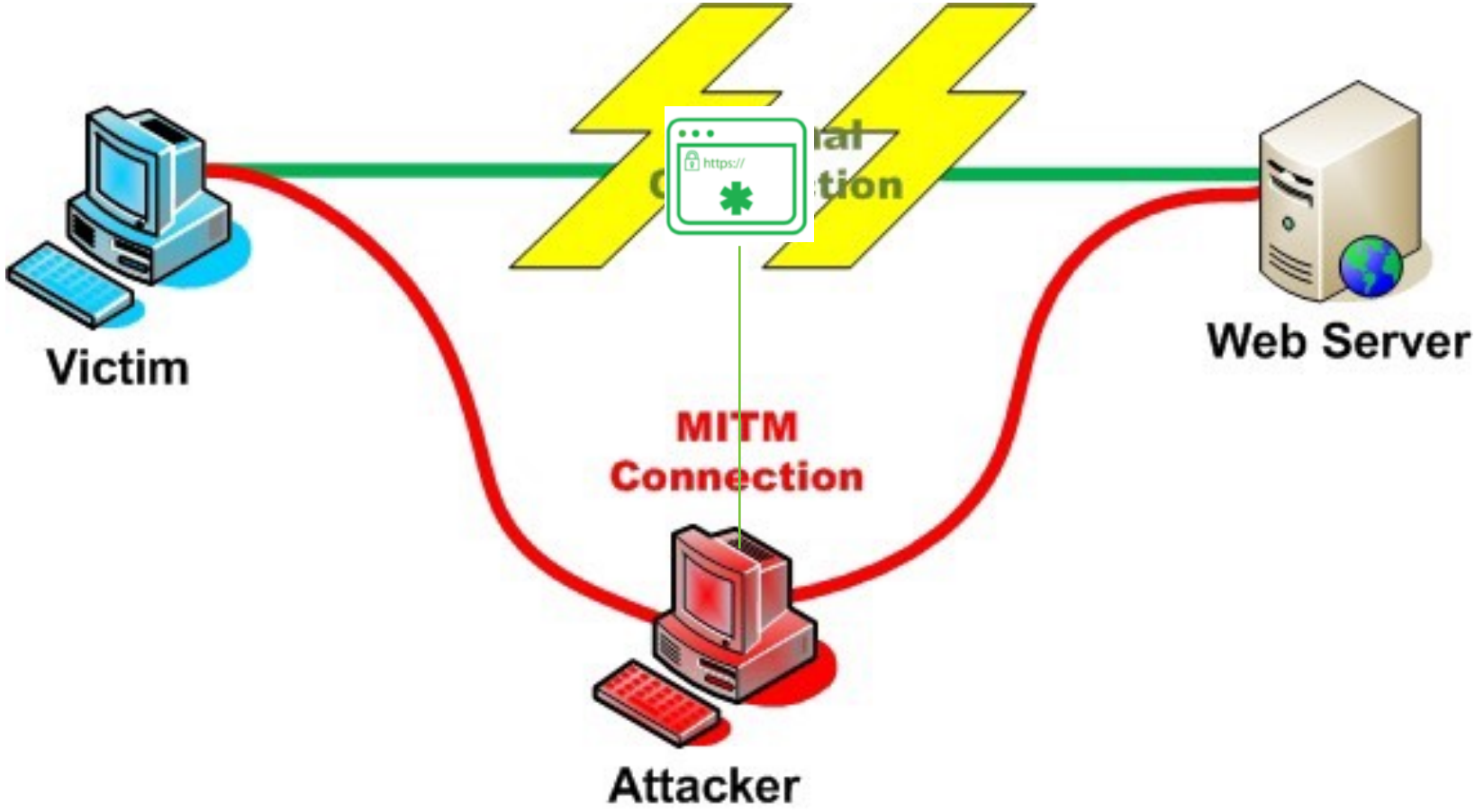




sedian Seguridad Digital de Andalucía

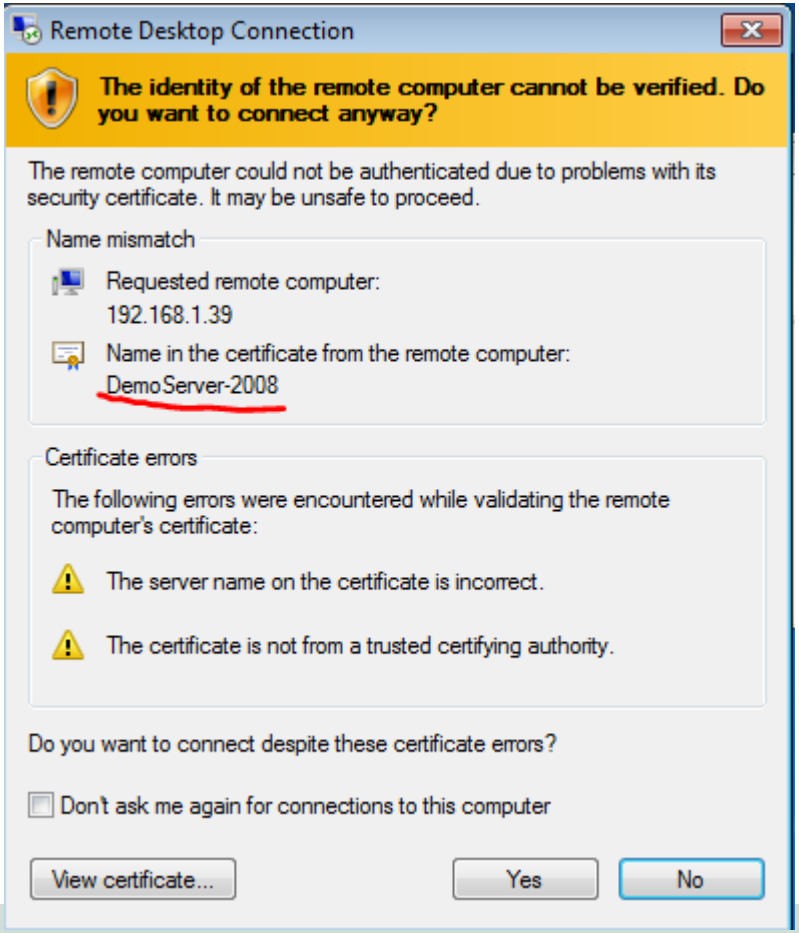
Otros ataques RDP

- Man in the Middle (Hombre en el medio traducido literalmente)

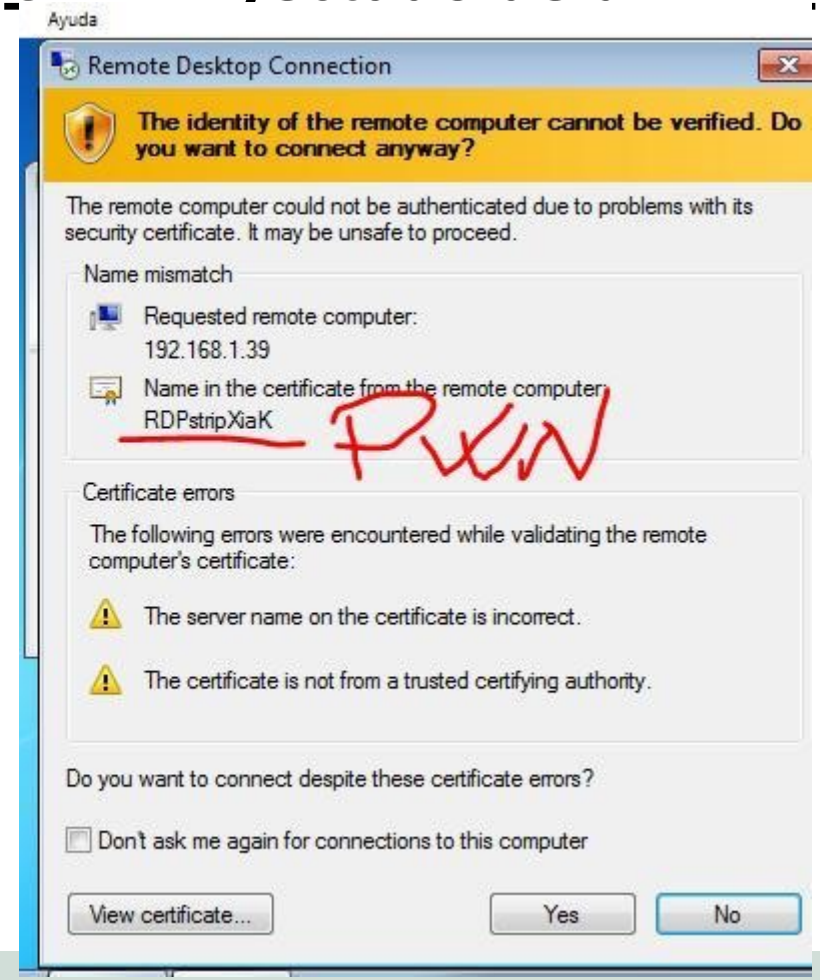


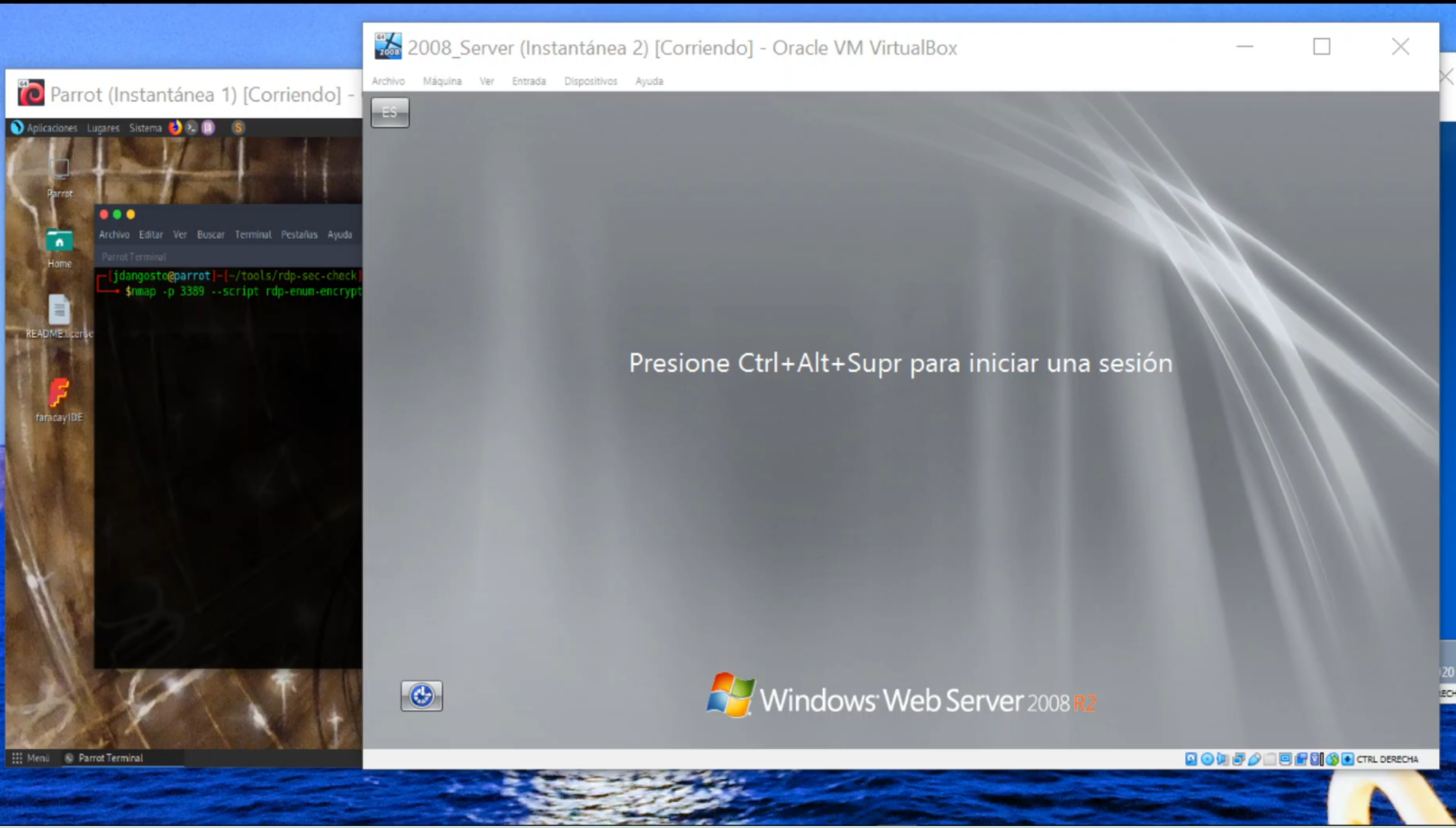
Man/Cert in the middle

CERT legítimo de un RDP



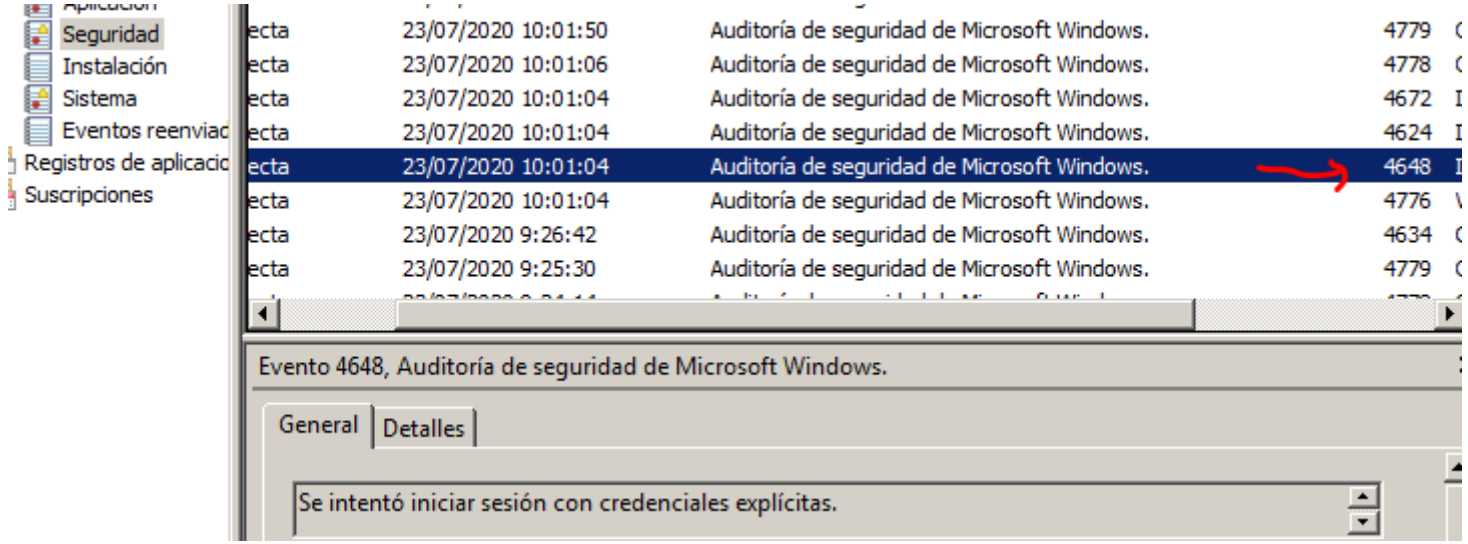
CERT invectado de un RDP





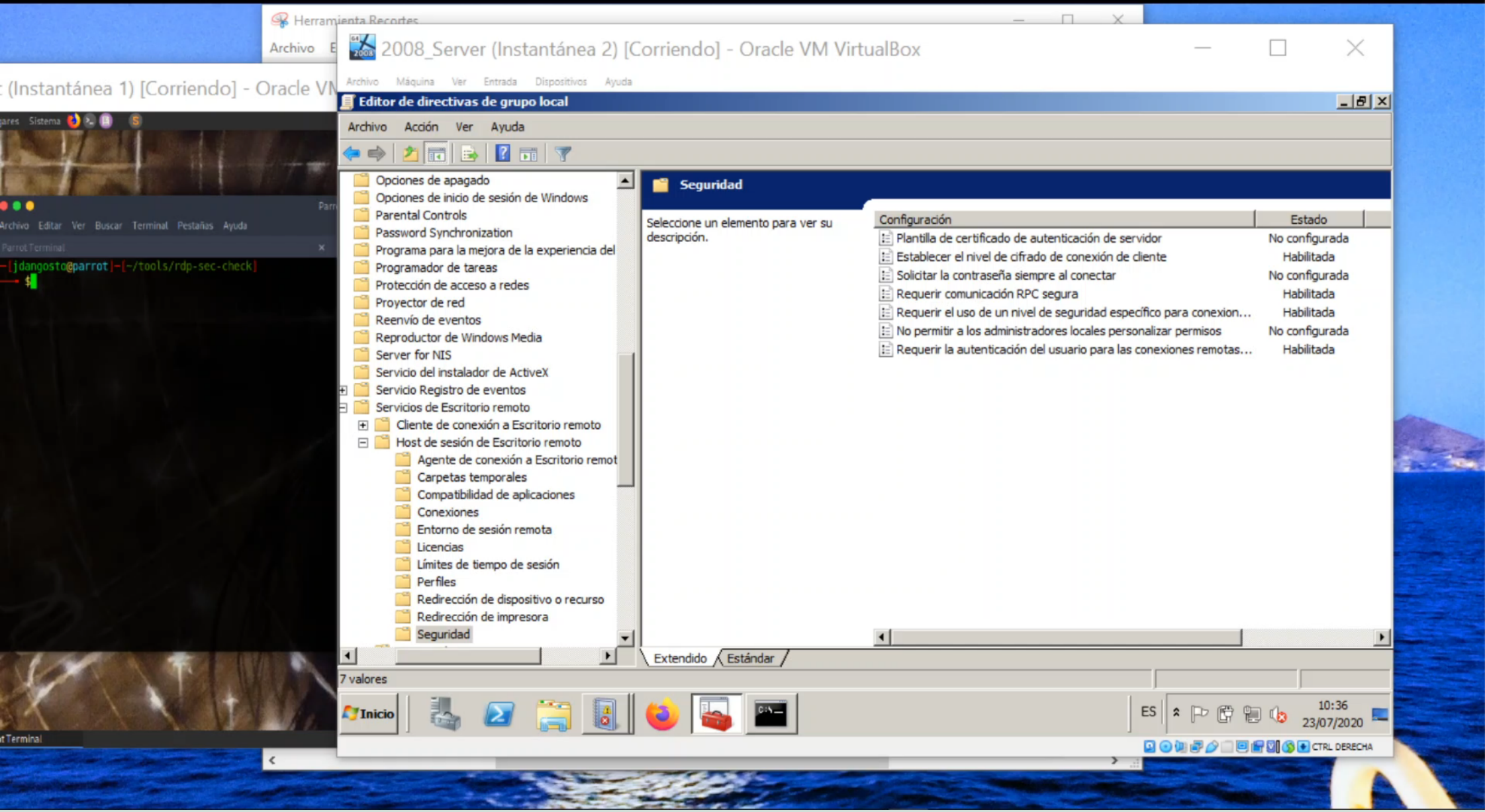
sedian Seguridad Digital de Andalucía

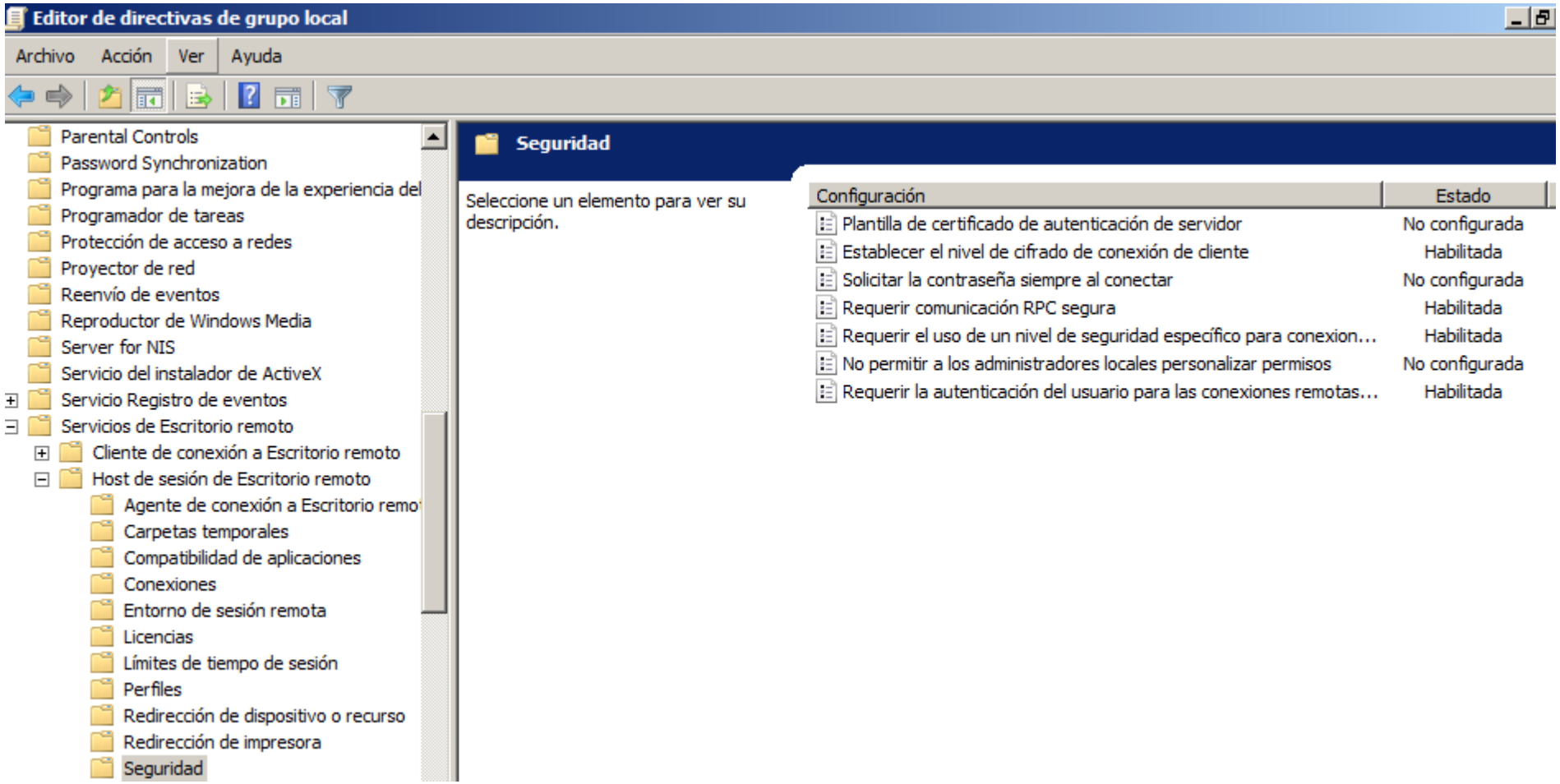
Eventos del sistema tras MITM



SubjectUserName DEMOSERVER-2008$
SubjectDomainName WORKGROUP
SubjectLogonId 0x3e7
LogonGuid {00000000-0000-0000-0000-000000000000}
TargetUserName Administrador
TargetDomainName DEMOSERVER-2008
TargetLogonGuid {00000000-0000-0000-0000-000000000000}
TargetServerName localhost
TargetInfo localhost
ProcessId 0x3c0
ProcessName C:\Windows\System32\winlogon.exe
IpAddress 192.168.1.66
IpPort 59142

¿Es posible bloquear un ataque de MITM sobre RDP?


Herramienta Recortes
Archivo
2008_Server (Instantánea 2) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Editor de directivas de grupo local
Archivo Acción Ver Ayuda
Opciones de apagado
Opciones de inicio de sesión de Windows
Parental Controls
Password Synchronization
Programa para la mejora de la experiencia del
Programador de tareas
Protección de acceso a redes
Proyector de red
Reenvío de eventos
Reproductor de Windows Media
Server for NIS
Servicio del instalador de ActiveX
Servicio Registro de eventos
Servicios de Escritorio remoto
Cliente de conexión a Escritorio remoto
Host de sesión de Escritorio remoto
Agente de conexión a Escritorio remot
Carpetas temporales
Compatibilidad de aplicaciones
Conexiones
Entorno de sesión remota
Licencias
Límites de tiempo de sesión
Perfiles
Redirección de dispositivo o recurso
Redirección de impresora
Seguridad
Seguridad
Seleccione un elemento para ver su descripción.
Configuración
Estado
Plantilla de certificado de autenticación de servidor
No configurada
Establecer el nivel de cifrado de conexión de cliente
Habilitada
Solicitar la contraseña siempre al conectar
No configurada
Requerir comunicación RPC segura
Habilitada
Requerir el uso de un nivel de seguridad específico para conexion...
Habilitada
No permitir a los administradores locales personalizar permisos
No configurada
Requerir la autenticación del usuario para las conexiones remotas...
Habilitada
Extendido
Estándar
7 valores
Inicio
ES
10:36
23/07/2020
CTRL DERECHA
(Instantánea 1) [Corriendo] - Oracle VM
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
Parrot Terminal
[jdangosto@parrot]-[~/tools/rdp-sec-check]


Editor de directivas de grupo local
Archivo
Acción
Ver
Ayuda
Parental Controls
Password Synchronization
Programa para la mejora de la experiencia del
Programador de tareas
Protección de acceso a redes
Proyector de red
Reenvío de eventos
Reproductor de Windows Media
Server for NIS
Servicio del instalador de ActiveX
Servicio Registro de eventos
Servicios de Escritorio remoto
Cliente de conexión a Escritorio remoto
Host de sesión de Escritorio remoto
Agente de conexión a Escritorio remo
Carpetas temporales
Compatibilidad de aplicaciones
Conexiones
Entorno de sesión remota
Licencias
Límites de tiempo de sesión
Perfiles
Redirección de dispositivo o recurso
Redirección de impresora
Seguridad
Seguridad
Seleccione un elemento para ver su descripción.
Configuración
Estado
Plantilla de certificado de autenticación de servidor
No configurada
Establecer el nivel de cifrado de conexión de cliente
Habilitada
Solicitar la contraseña siempre al conectar
No configurada
Requerir comunicación RPC segura
Habilitada
Requerir el uso de un nivel de seguridad específico para conexion...
Habilitada
No permitir a los administradores locales personalizar permisos
No configurada
Requerir la autenticación del usuario para las conexiones remotas...
Habilitada

sedian Seguridad Digital de Andalucía