

Joel Gámez Molina

▶ HackPlayers

@JoelGMSec

AutoRDPwn: The Shadow Attack Framework











whoami Joel Gámez Molina

- Administrador de sistemas durante 10 años
- Ex-Director técnico de Cyberguard
- Actualmente Security Analyst en Deloitte
- Creador y escritor del blog darkbyte.net
 - https://twitter.com/JoelGMsec
 - https://github.com/JoelGMSec
 - https://ko-fi.com/JoelGMSec









ATENCIÓN!



OJO CUIDAO!





Disclaimer

- No soy programador
- Es un proyecto personal
- Se trata de una idea original
- Apto para casi todos los públicos
- Tengo que dar por hecho muchas cosas
- No hagáis cosas malas

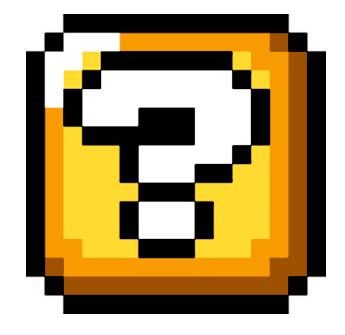








VALE, MUY BIEN



PERO DE QUÉ VA ESTO?







REMOTE DESKTOP



PROBLEM PROTOCOL





Ataques a RDP

- Brute Force
- Denial of Service
- Privilege Escalation
- Command Execution
- Man in The Middle
- Session Hijacking

- CVE-2017-0176
- CVE-2017-8673
- CVE-2018-0886
- CVE-2018-0976
- CVE-2019-0708
- CVE-2019-1223





BRUTE FORCE

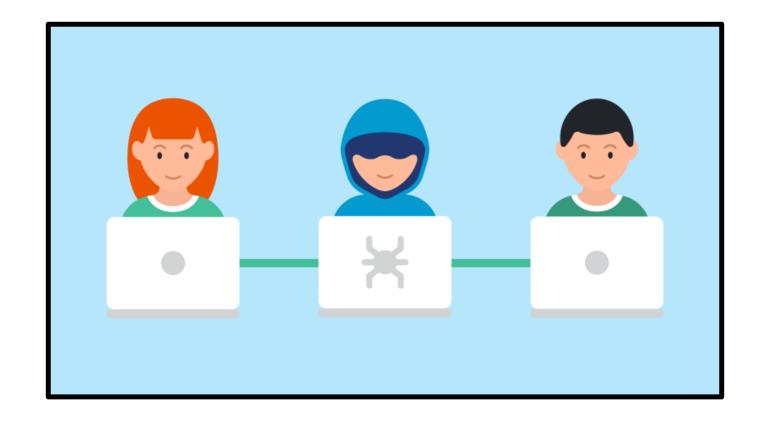








MAN IN THE MIDDLE

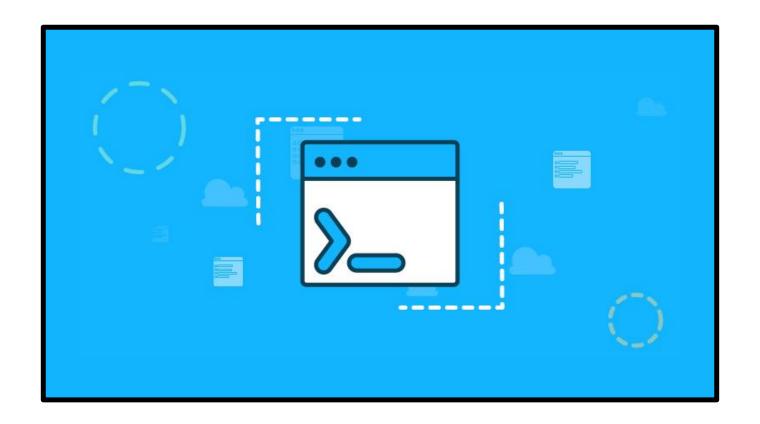








SESSION HIJACKING

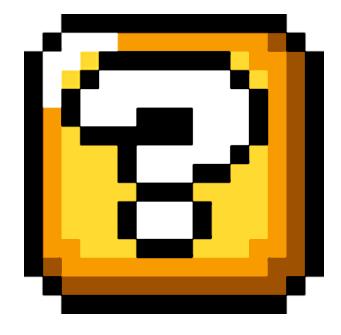








QUÉ SON LAS



SHADOW SESSIONS?







Shadow Sessions

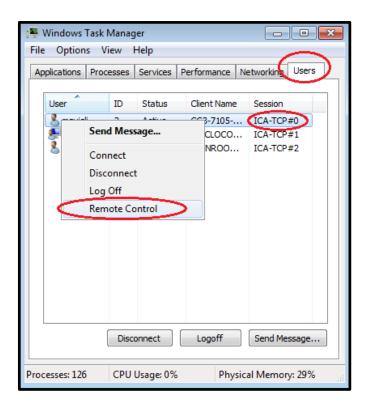
- Es una característica especial de Terminal Services
- Su cometido es dar soporte a los usuarios
- Se incorporó en Windows Server 2003
- Existen 5 niveles de configuración diferentes
- Lo deshabilitaron en Windows Server 2012
- Lo volvieron a habilitar en Windows Server 2012 R2

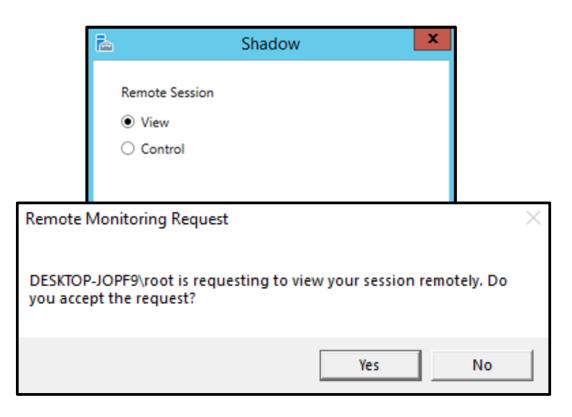






Shadow Sessions









Shadow Sessions

		E Sur	nend user sign-in to so	molete ann registr	ration	Not configured	No	
Event Viewer	 Suspend user sign-in to complete app registration Set rules for remote control of Remote Desktop Services use 					Not configured	No	
Family Safety					The second secon	H-5-		
			ect network detection o	n the server		Not configured	No	
File History			<u>\$</u>	et rules for ren	note control o	f Remote Deskt	op Services user sessions	
Game Explorer		Re					O 2000	
HomeGroup		Al Set rules for remote control of Remote Desktop Ser				ices user sessions	Previous Setting Next Settin	
		ΞTυ	700					
Internet Information Services			O Not Configured	Comment:				
			O Not Configured					
Maintenance Scheduler			Enabled					
NetMeeting			O 8: 11-1					
Network Access Protection			O Disabled	Connected				
Network Projector	=			Supported on:			Server 2008, Windows Server 2003, W	
OneDrive					Windows Vista,	and Windows XP		
Online Assistance								
Password Synchronization			Options:			Help:		
Portable Operating System								
Presentation Settings			Options:				policy setting, administrators can into	
Remote Desktop Services						a user's Remote Desktop Services session based on the selected. Select the desired level of control and permiss		
RD Licensing		No remote control allowed						
Remote Desktop Connection Client		No remote control allowed the options list:						
Remote Desktop Session Host		Full Control with user's permission					rol allowed: Disallows an administrat	
Application Compatibility		View Session with user's permission View Session with user's permission View Session with user's permission						
Connections		View Session without user's permission 2. Full Control with user's permission: Allows the admit						
Device and Resource Redirection		interact with the session, with the user's consent. 3. Full Control without user's permission: Allows the						
Licensing							iteract with the session, without the i	
Printer Padiroction						danimistrator to in	teroce with the session, without the	







The Shadow Attack

- No se trata de un ataque como tal
- Está catalogado como característica por Microsoft
- Funciona en todas las versiones de Windows
- No cerramos ni robamos la sesión en ningún momento
- No es necesario instalar nada, es nativo del sistema
- La conexión utiliza puertos aleatorios (a través de RPC)







The Shadow Attack

Fase 1

- Habilitar el escritorio remoto en la víctima
- Habilitar las Shadow Sessions (GPO/Regedit)
- Deshabilitar protecciones (CredSSP, NLA, Firewall..)

Fase 2

- Deshabilitar el consentimiento del usuario
- Configurar las reglas de control de la sesión
- Fun and profit!







Automatizamos?

- Crear una herramienta fácil y sencilla
- Que disponga de diferentes vectores de ataque
- Que sea modular y parametrizable
- Que incorpore técnicas de evasión
- Que sea compatible con Windows y Linux
- Que se ejecute en memoria y no tenga dependencias







Así empezó todo



- [1] Lanzar el ataque a través de PsExec
- [2] Lanzar el ataque a través de WMI
- [3] Cerrar el programa

Elige la opción que más te interese:





Algunas mejoras

- Bypass de UAC y AMSI
- Autodetección de ld de sesión
- Exclusiones en Windows Defender
- Limpieza automática del script
- Ejecución remota mejorada
- Módulos adicionales y ataques nuevos









```
:: The Shadow Attack Framework :: v5.0 :: Created by @JoelGMSec ::
[1] - PSexec (SMB)
   - Pass the Hash (SMB)
[3] - Windows Management Instrumentation (WMI)
[4] - Windows Remote Management (WinRM)
[5] - Windows Remote Assistance (WinRS)
[6] - Local Session Hijacking (TSCon)
   - Remote Desktop Execution (RDP)
   - Cargar módulos adicionales
[X] - Cerrar el programa
```

Elige cómo quieres lanzar el ataque: _





Vectores de ataque

- PSexec (SMB)
- Pass the Hash (SMB)
- Windows Management Instrumentation (WMI)
- Windows Remote Management (WinRM)
- Windows Remote Assistance (WinRS)
- Local Session Hijacking (TSCon)
- Remote Desktop Execution (RDP)



Módulos adicionales

- Netcat & WinRS
- Mimikatz
- SharpWeb
- TCP Port Scanner
- Local Port Forwarding
- Powershell Web Server

- Remote Desktop Forensics
- Sticky Keys Hacking
- Metasploit Web Delivery
- Remote Keylogger
- Privilege Escalation
- Remote VNC Server











L'osas por hacer

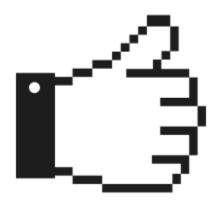
- Reescribir todo el código desde cero
- Hacer reversible todo el proceso en la víctima
- Añadir ofuscación y cifrado para evadir AV/IDS/IPS
- Compatibilidad completa con Linux a través de docker
- Habilitar la ejecución local o remota de los módulos
- Lanzar el ataque de forma masiva a través de la red







Gracias! Preguntas?







Hackplayers conference

Sending SIGKILL to all processes.
Please stand by while rebooting the system.
[64857.521348] sd 0:0:0:0: [sda] Synchronizing SCSI cache
[64857.522838] Restarting system.

_