HackPlayers
c0nference
www.h-c0n.com

Joel Gámez Molina @JoelGMSec

AutoRDPwn: The Shadow Attack Framework

Hackplayers c0nference MMXX

LA NAVE

whoami

Joel Gámez Molina

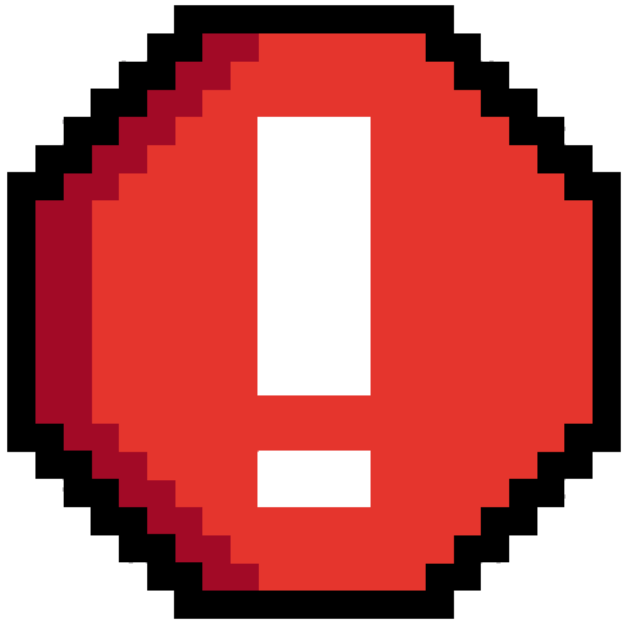
- Administrador de sistemas durante 10 años
- Ex-Director técnico de Cyberguard
- Actualmente Security Analyst en Deloitte
- Creador y escritor del blog darkbyte.net

https://twitter.com/JoelGMsec

https://github.com/JoelGMSec

https://ko-fi.com/JoelGMSec

ATENCIÓN!



OJO CUIDAO!

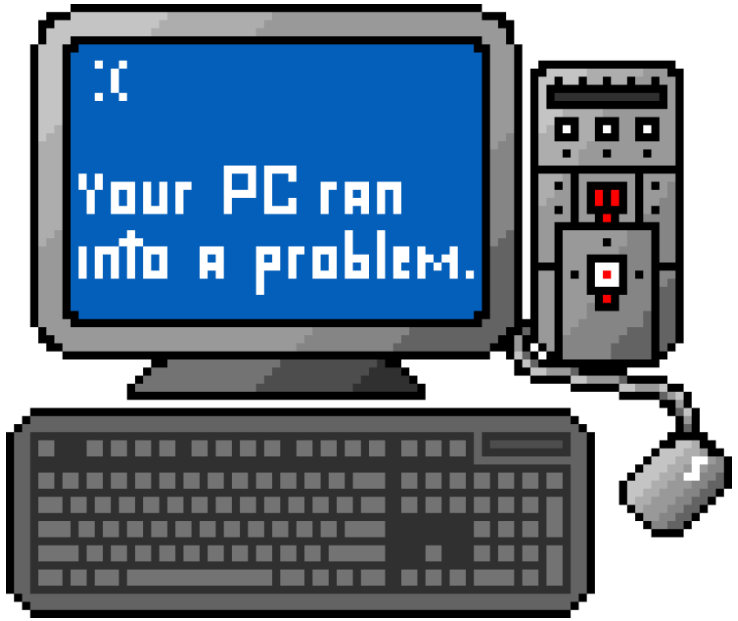
Disclaimer

- 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

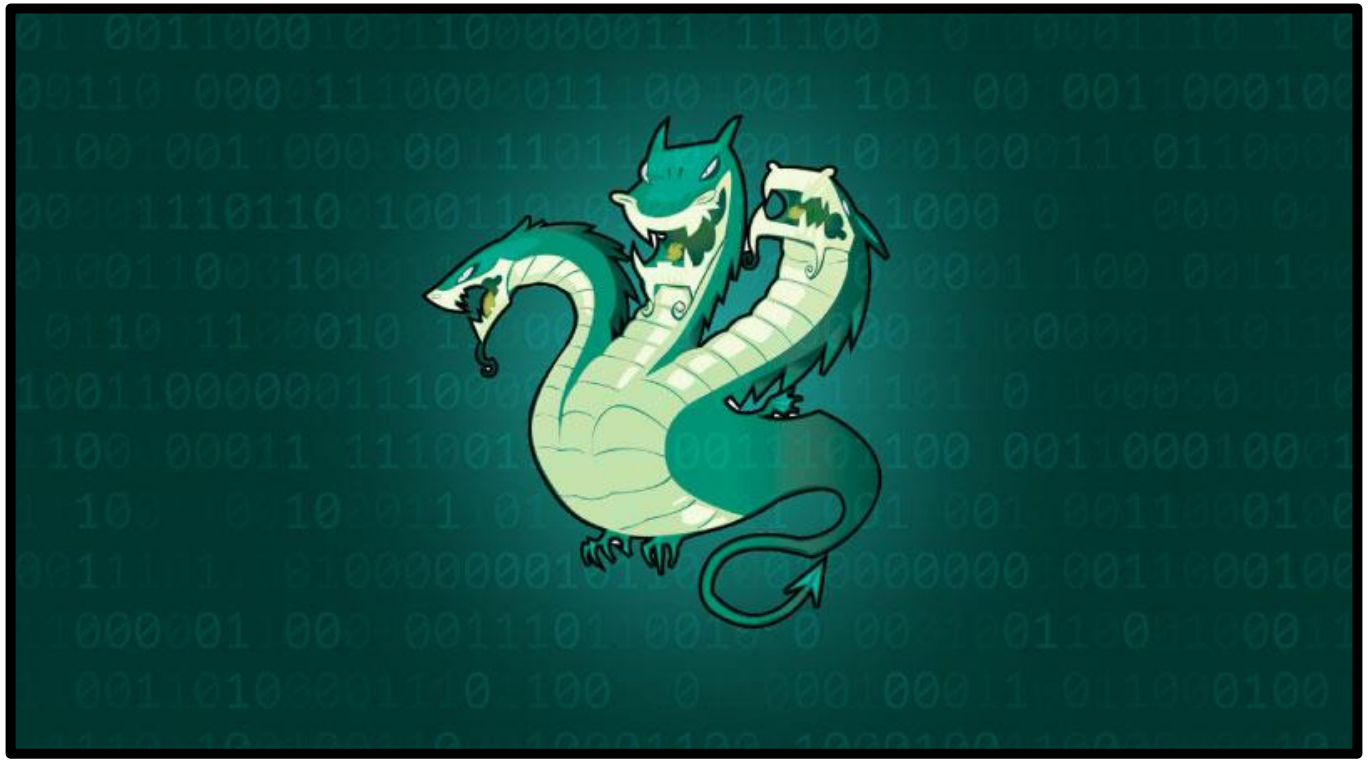


PROBLEM PROTOCOL

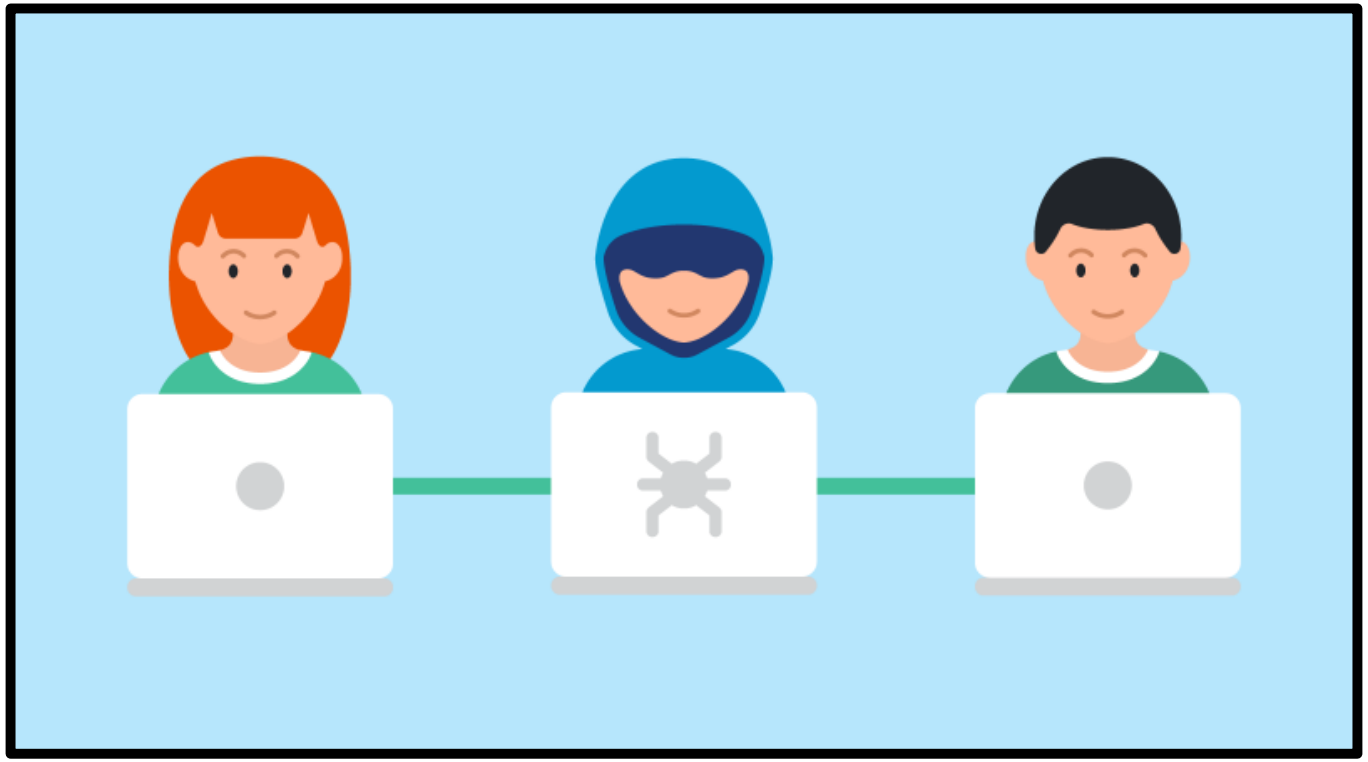
Ataques a RDP

- 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

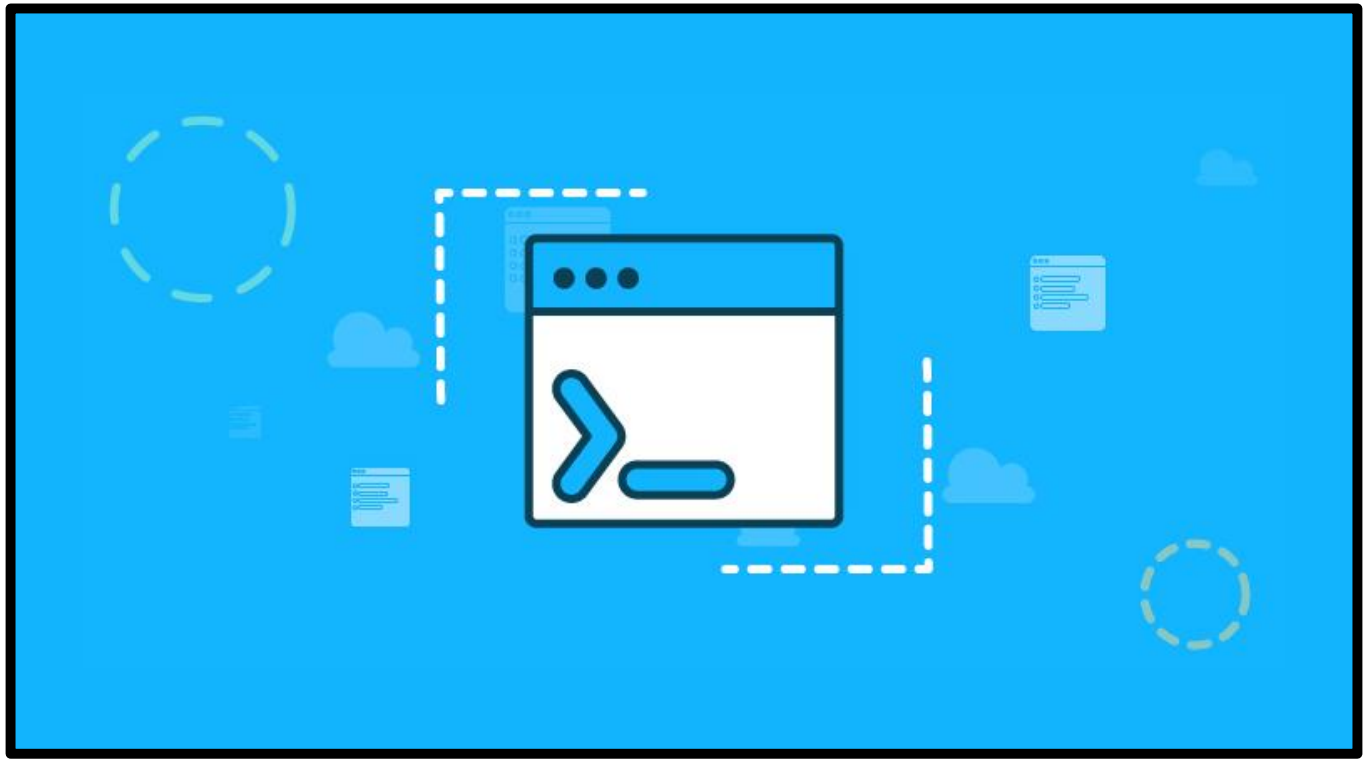
BRUTE FORCE



MAN IN THE MIDDLE



SESSION HIJACKING



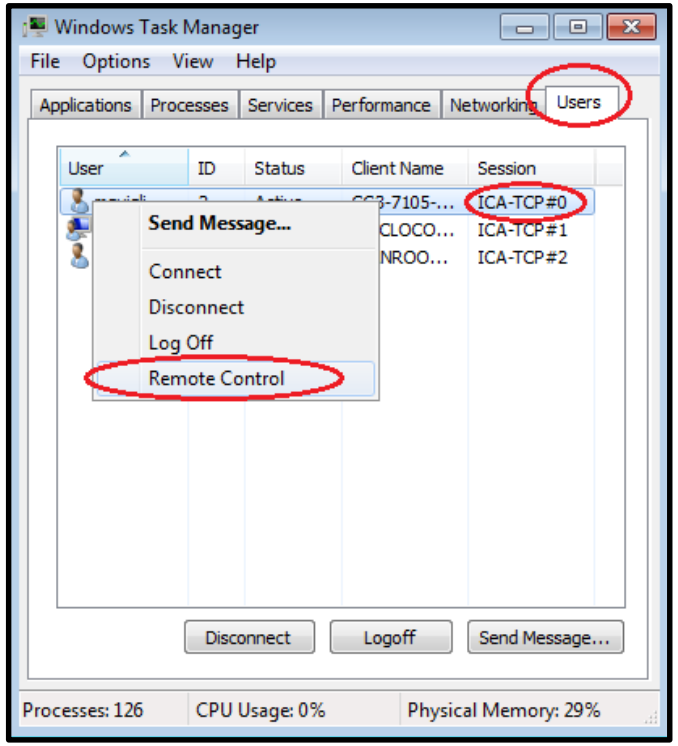
QUÉ SON LAS

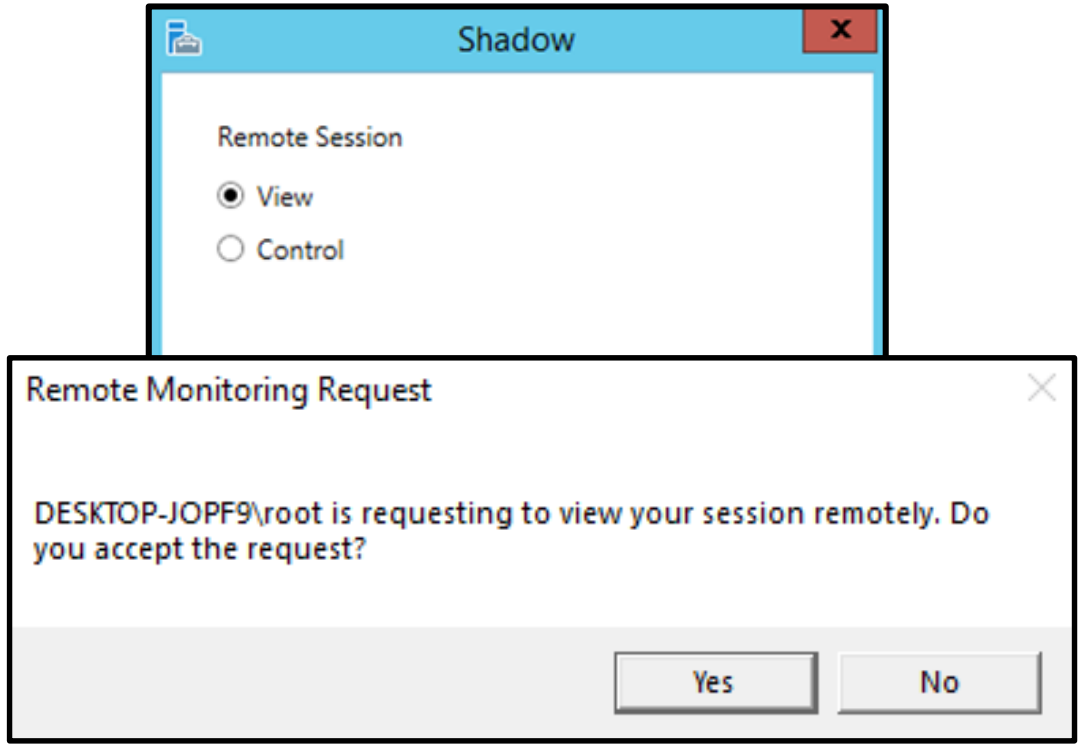
SHADOW SESSIONS?

Shadow Sessions

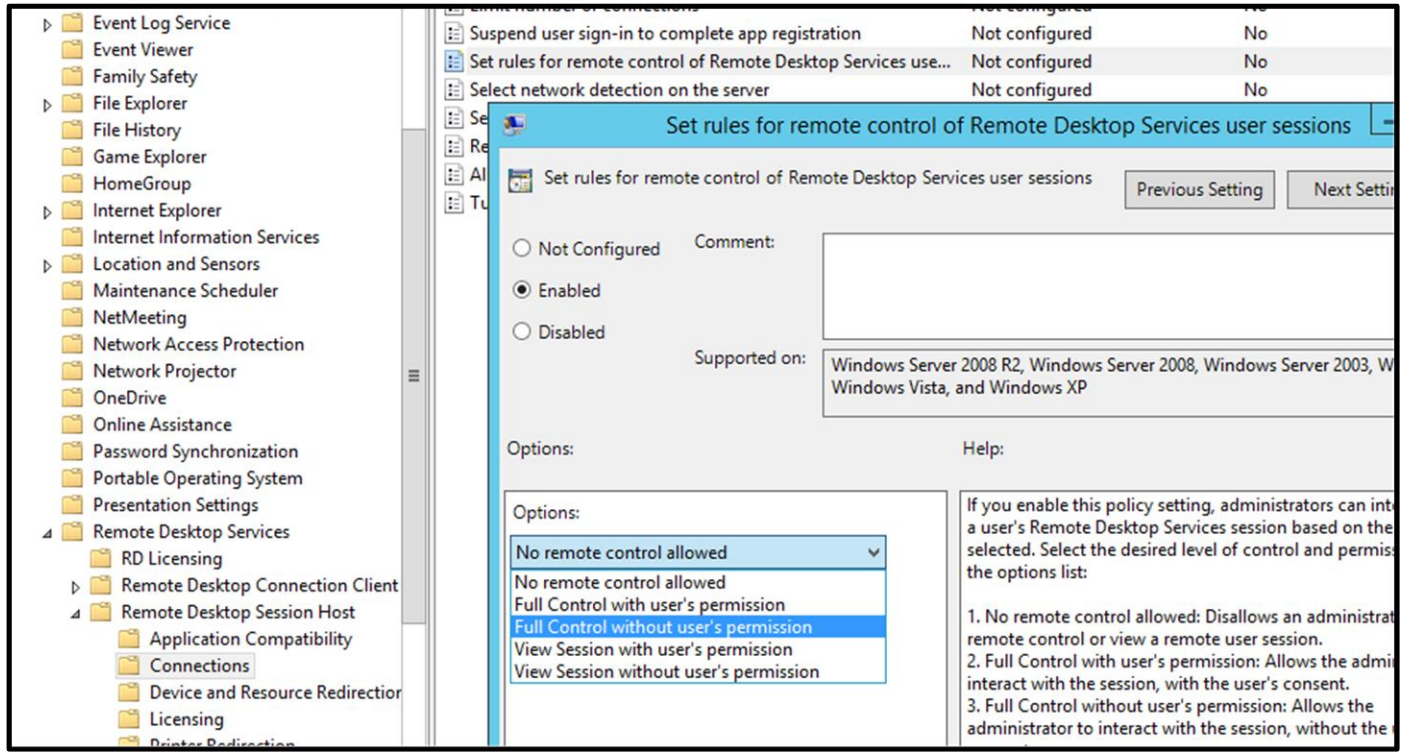
- Es una característica especial de Terminal Services
- Su cometido es dar soporte a los usuarios
- Se incorporó en Windows Server 2003
- Existen 5 niveles de configuración diferentes
- Lo deshabilitaron en Windows Server 2012
- Lo volvieron a habilitar en Windows Server 2012 R2

Shadow Sessions





Shadow Sessions



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..)

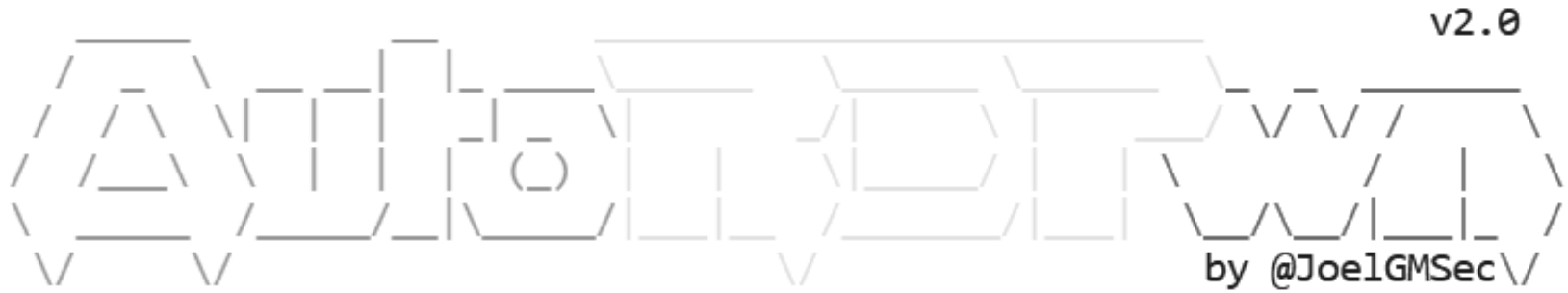
Fase 2

- 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 Id 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)
[2] - Pass the Hash (SMB)
[3] - Windows Management Instrumentation (WMI)
[4] - Windows Remote Management (WinRM)
[5] - Windows Remote Assistance (WinRS)
[6] - Local Session Hijacking (TSCon)
[7] - Remote Desktop Execution (RDP)
[M] - 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

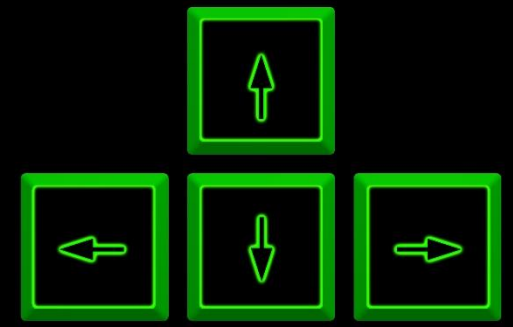

LET'S PLAY!

Cosas 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?



> h-c0n

Hackplayers c0nference

```
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.
_
```

www.h-c0n.com