AutoRDPwn:

The Shadow Attack Framework

whoami

Joel Gámez Molina

(aka @JoelGMSec)

- System Administrator for +10 years
- Former Cyberguard Technical Director
- Currently Security Analyst at Deloitte
- Creator and writer of the blog darkbyte.net

twitter.com/JoelGMsec

github.com/JoelGMSec

mypublicinbox.com/JoelGMSec

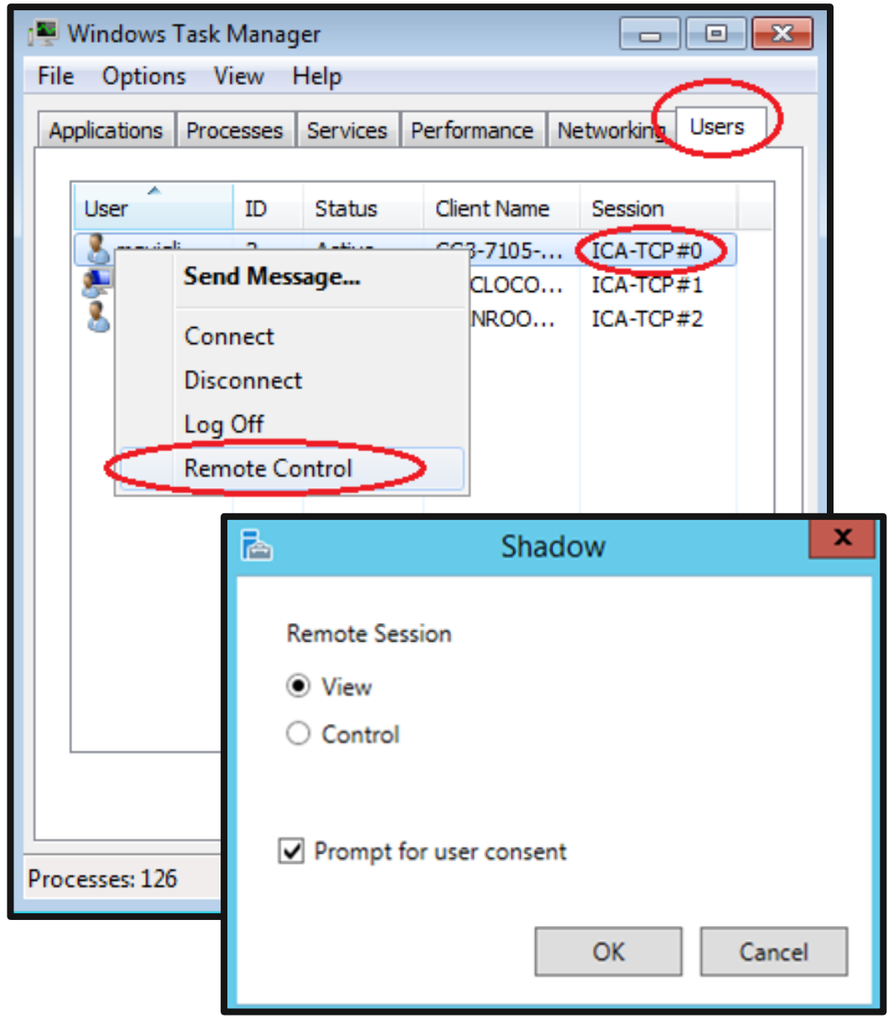
Disclaimer

- I'm not a programmer
- ~~It's~~ a personal project
- This is an original idea
- Suitable for almost all audiences
- I have to take a lot of things for granted
- Don't do bad things 😇 😈

What are the Shadow Sessions ?

Shadow Sessions

- This is a special feature of Terminal Services
- Its mission is to support users
- Built into Windows Server 2003
- There are 5 different configuration levels
- They disabled it in Windows Server 2012
- They re-enabled it in Windows Server 2012 R2



The Shadow Attack

- This is not an attack as such
- It is listed as a feature by Microsoft
- Works on all versions of Windows
- We don't log off or steal the session at any time
- No need to install anything, it's native to the system
- The connection uses random ports (via RPC)

Attack Vectors

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

Additional modules

- Netcat & WinRS
- Mimikatz
- SharpWeb
- TCP Port Scanner
- Local Port Forwarding
- Powershell Web Server
- Remote Desktop Forensics
- Sticky Keys Hacking
- Metasploit Reverse Shell
- Remote Keylogger
- Privilege Escalation
- Remote VNC Server

:) DEMO

Your PC is perfectly stable and is running with absolutely no problems whatsoever.

1000% Complete

For more information about this tool, visit https://github.com/JoelGMSec/AutoRDPwn

You can search for this status code online if you'd like:
Stop code: ALL_SYSTEMS_GO

Things to do

- Rewrite all the code from scratch
- Make the whole process reversible in the victim
- Add obfuscation and encryption to evade AV/IDS/IPS
- Full Linux support via docker
- Enable local or remote execution of modules
- Launching the attack massively through the network

Thank you!

Questions?