

Attacking Targets with Metasploit

INVESTIGATING THE METERPRETER PAYLOAD



Kevin Cardwell

PRESIDENT, CYBER2ALBS LLC

www.cyber2labs.com



Overview



Explore the power of Meterpreter

Identify methods for persistence

Leverage extensions



Meterpreter



Powerful Shell



Fileless

Advanced file manipulation

Encrypted

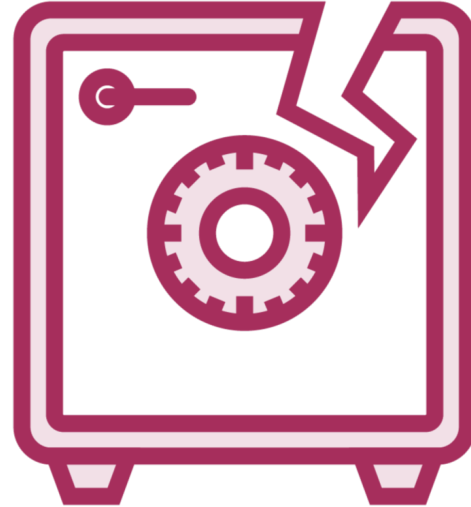
Migration

Pivoting

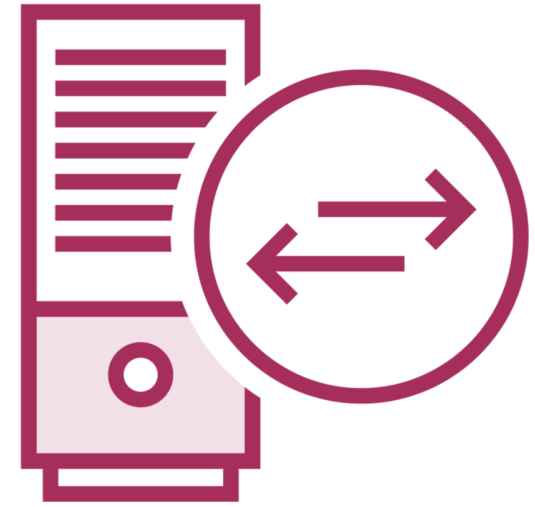
Features



Injection



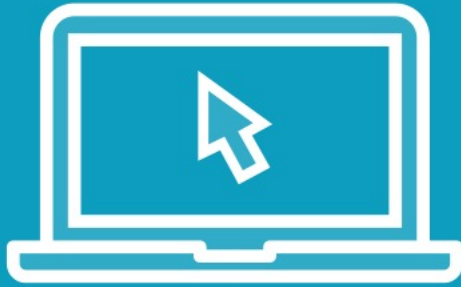
Exfiltration



Port-Forwarding



Demo



Power of Meterpreter



Identify Methods of Persistence



Maintain Access

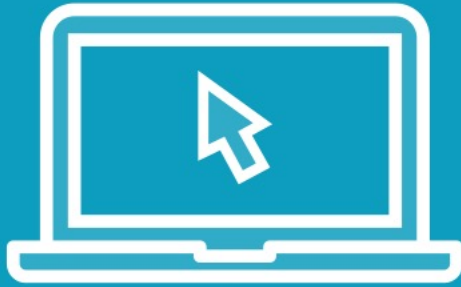


Callbacks



RAT

Demo



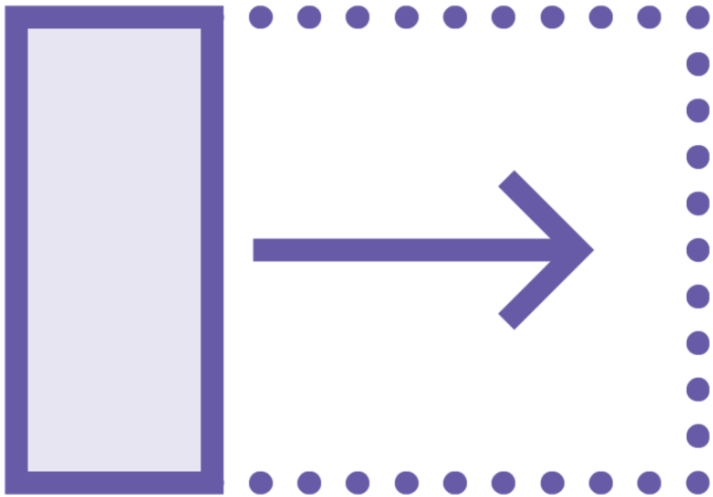
Persistence



Extensions



Expansion



Powershell

Mimikatz

Application Programming Interface calls

More



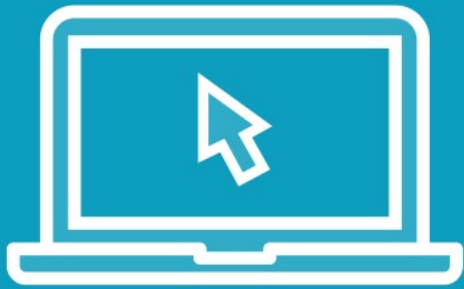
Keyloggers



Controls



Demo



Extensions



Summary



Explored the power of Meterpreter
Identified methods for persistence
Leveraged extensions

