

Searching and Exfiltrating Sensitive Data



Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant



Exfiltrating sensitive data
without being detected



Module Scenario



With admin rights and persistence, it is time to search and exfiltrate sensitive data

Show to our client the impact that a real hack could have



Module Overview



Techniques for data exfiltration

How to be stealthy

Search and exfiltrate sensitive files

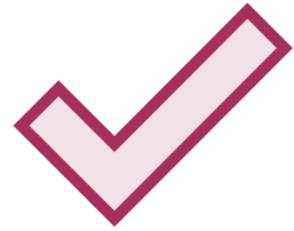
Getting microphone/webcam recordings

Keyloggers

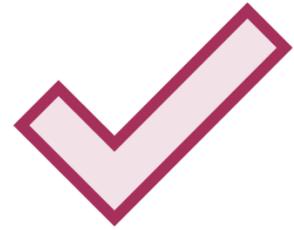
Course Closure



Techniques for Data Exfiltration



Transfer via Meterpreter to your server



Transfer via HTTPS, SFTP or SCP



Email attachments



Upload to a cloud storage



Avoiding Detection



Being as stealthy as possible to not be detected

Encrypting the files to be exfiltrated to avoid DLP tools

Sending the files using normal protocols

Blending exfiltration with regular traffic

Using whitelisted cloud services



Gathering Sensitive Files, Audio and Webcam



Legal Considerations



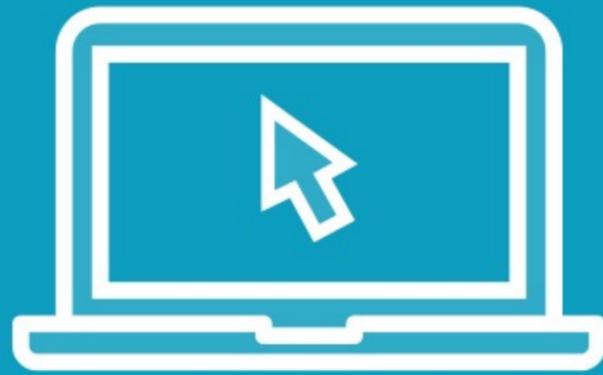
Recording audio/video without consent is illegal in most of the countries

Check in your country if you can do that, and get formal approval from your client

Stay out of trouble!



Demo



Gathering sensitive files

Recording audio/webcam

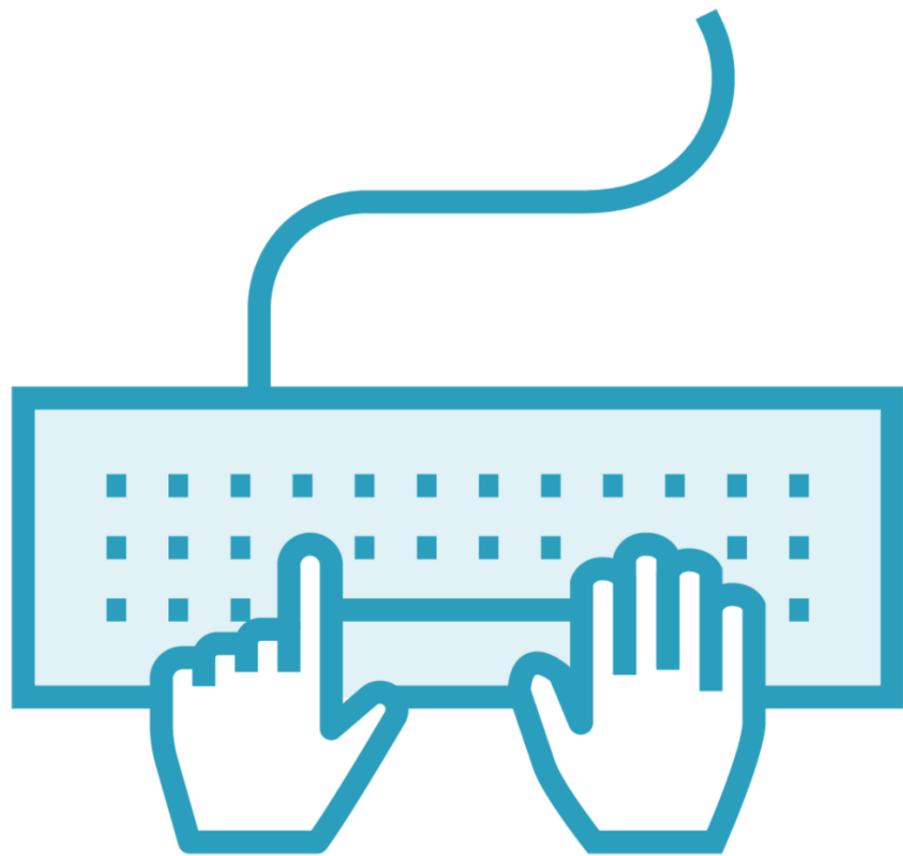
Taking screenshots



Keyloggers



Keyloggers with Meterpreter



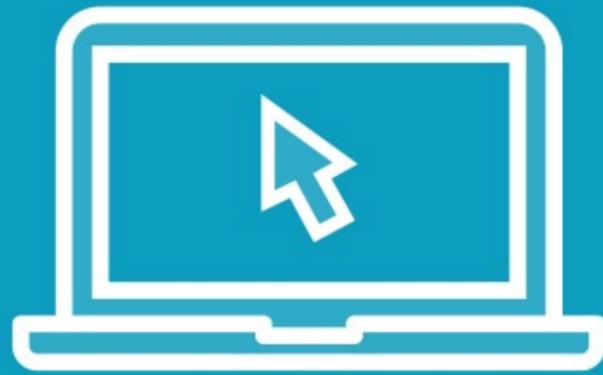
Meterpreter has an out-of-the-box keylogger

You enable the feature, and later go collect the keystrokes

Might be illegal, check with your laws and get client approval



Demo



Using the Meterpreter keylogger

Cleaning up your tracks



Course Closure



What You Learned



What Meterpreter is and how it works



How to get Meterpreter shells



Several techniques for privilege escalation



Several techniques for maintaining persistence



How to exfiltrate data in a stealthy way



How To Get the Most Out of This Course

**Practice the skills
you learned**

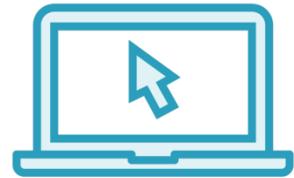
Course lab

**Review the Metasploit and
Meterpreter manuals**

**Try exploiting different
machines and OS**



What's Next



Course lab

Post Exploitation with Meterpreter Lab



Practice on live environments

hackthebox.eu | pentestit.ru



Red team tools courses at Pluralsight

pluralsight.com/paths/skill/red-team-tools



Next Meterpreter course

Defense Evasion with Meterpreter



Thank you!



Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant

