

Creating Persistence



Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant



Accessing your
victim computer at anytime



Module Scenario



With admin-level access to the target machine, now it is time to create persistence

Create backdoors so we can access the system at anytime we want, even if the vulnerability is patched

Real world pentest: make sure you have formal approvals for backdoors



Module Overview



Main techniques for persistence

Creating backdoor services and tasks

Creating additional backdoors



Ways of Creating Persistence

Backdoor services

Scheduled tasks

Hidden users

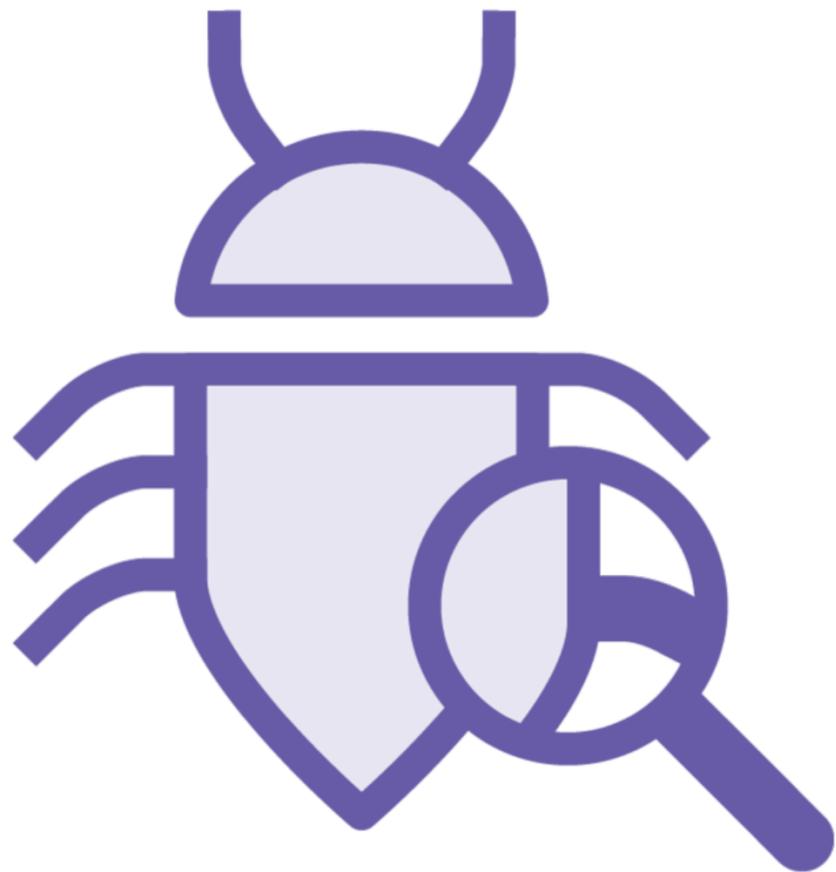
Legitimate software compromise



Creating Backdoor Services and Tasks



How Backdoor Services/Tasks Work



Making the victim computer automatically connect back to your Meterpreter server

Create a Meterpreter payload (initial stager)

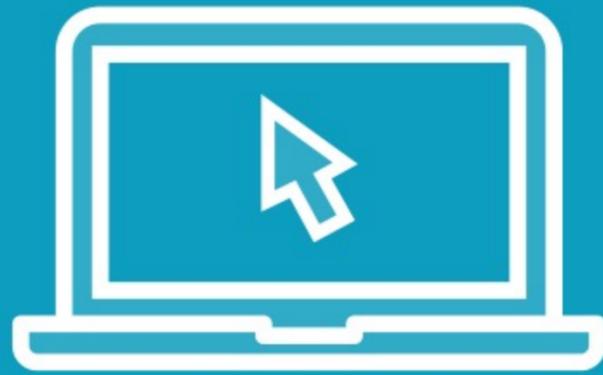
Create a service or schedule task that executes the Meterpreter payload

Be stealthy!

- **Evaluate what is already in the server**
- **Create something that is not suspicious and similar to the environment**
- **Payloads might be detected by anti virus**



Demo



Creating backdoors

- Malicious services
- Malicious scheduled tasks



Creating Other Backdoors



Other Backdoor Types



Several other ways of creating backdoors

Creating backdoor users

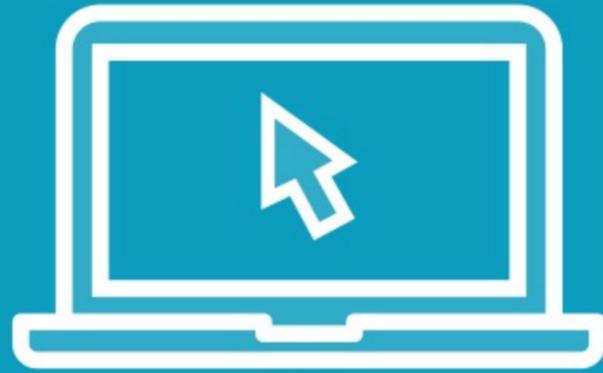
- Analyze the current environment
- Create a non-suspicious user

Infecting existing applications

- Find applications that are frequently used
- Infect the executable with a Meterpreter payload
- Might be lost in software updates



Demo



Creating additional backdoors

- Backdoor users
- Infecting legitimate software



Summary



What are the main ways of establishing persistence

How to create backdoor services and tasks with Meterpreter

How to create backdoor users

How to infect legitimate software to create persistence



Next up:
Searching and Exfiltrating
Sensitive Data

