

Privilege Escalation



Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant



Getting admin-level access



Module Scenario



With a low-level privilege Meterpreter shell, the objective is to get an admin level shell

- Exploit internal vulnerabilities**
- Find misconfigured services**



Module Overview



Main techniques for privilege escalation

How to find and exploit internal vulnerabilities

How to find and exploit misconfigured services

How to gather password hashes from a Windows machine



Ways of Escalating Privileges

Exploiting internal vulnerabilities

Exploiting misconfigurations

Finding username/passwords

Phishing credentials

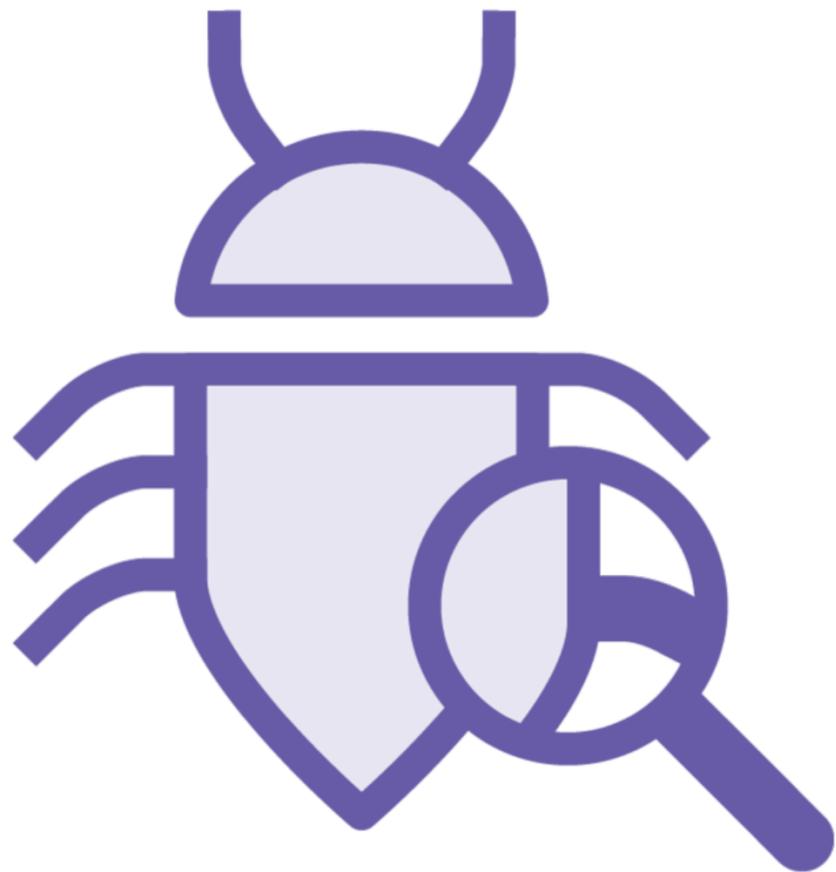
etc.



Privilege Escalation via Vulnerabilities



Exploiting Internal Vulnerabilities



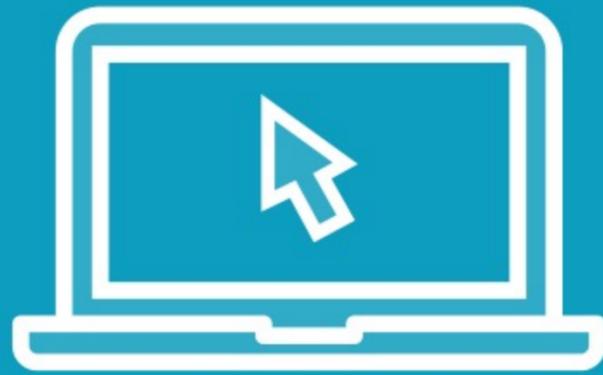
Services that are running as administrator or system

Vulnerabilities in services not exposed externally

Increased chance of getting detected if you are transferring exploits or payloads



Demo



Escalate privileges using a vulnerable service

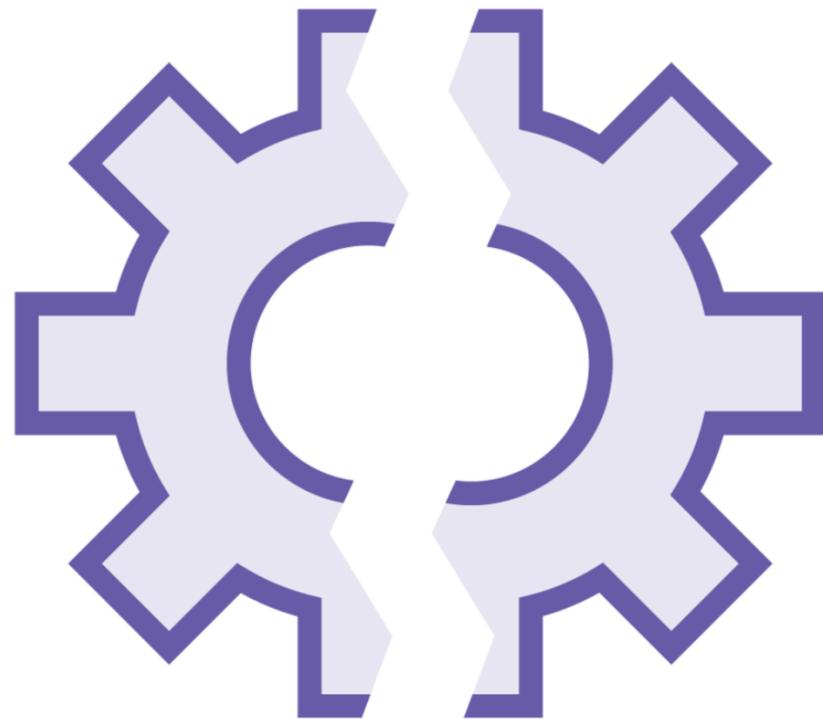
- Finding potential vulnerabilities
- Using “Exploit Suggester”
- Exploiting a vulnerability
- Using the Meterpreter GetSystem



Privilege Escalation Via Misconfigurations



Common Misconfigurations for Privilege Escalation

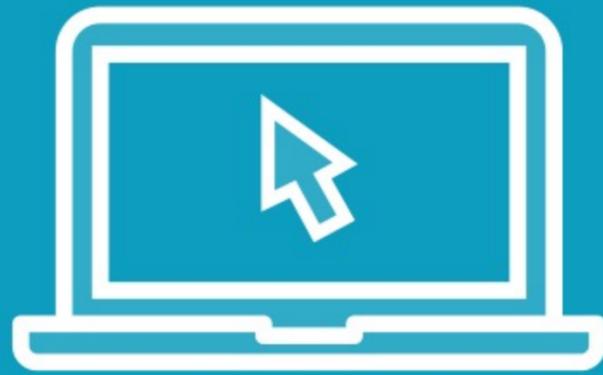


There are several types of misconfigurations that can be exploited to escalate privileges

- Services running as ADMIN but with files that can be changed by anyone**
- Scheduled tasks with wrong file permissions**
- Credentials in a script file**



Demo



Escalating privileges via misconfigurations

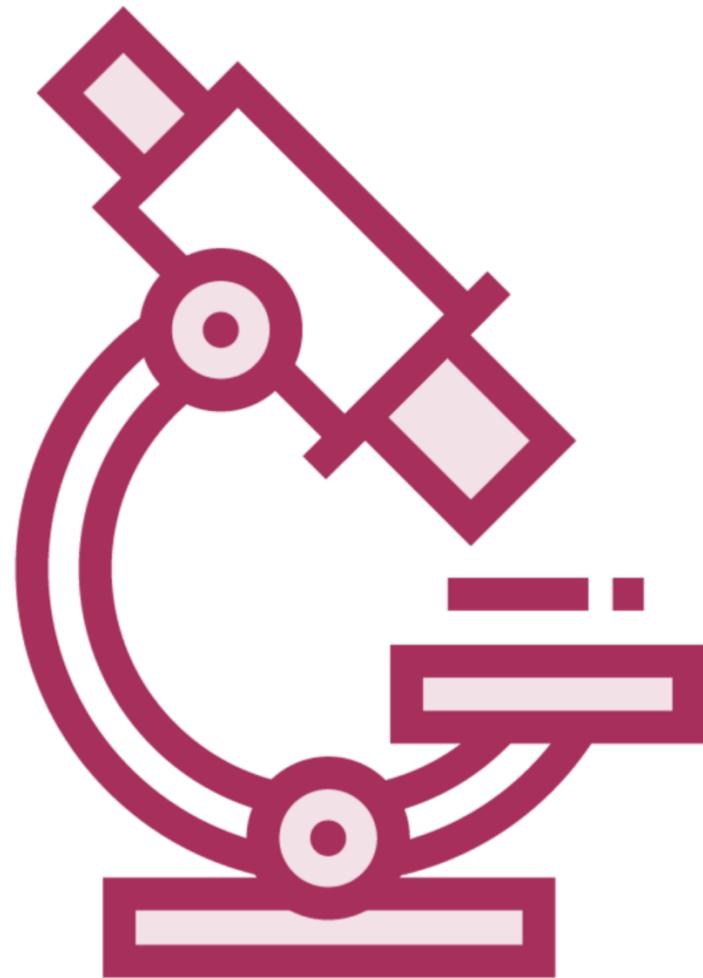
- Finding a misconfiguration
- Creating a malicious payload
- Getting an admin-level Meterpreter shell



Dumping Credential Hashes



How Meterpreter Gets Password Hashes



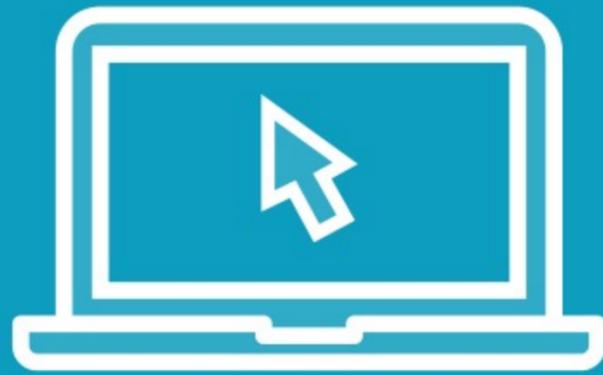
All user credentials are stored in disk

Passwords are encrypted/hashed

Meterpreter is able to find the stored hashes and generate a file to be used by cracking tools



Demo



Gathering password hashes from a Windows machine

- **Dump using Hashdump**



Summary



What are the main ways of achieving privilege escalation

How to find and exploit internal vulnerabilities with Meterpreter

How to exploit a misconfigured service

How to dump password hashes using Meterpreter



Next up:
Creating Persistence

