

# Active Directory Enumeration

---



**Ricardo Reimao, OSCP, CISSP**  
Cybersecurity Consultant



Gathering information about  
the domain



## Module Overview



**Understanding Active Directory enumeration**

**Enumerating domain users, computers, assets and much more**

**Working with Active Directory Service Interfaces (ADSI)**

**Retrieve service account hashes via Kerberoasting**



# Course Scenario: Globomantics Red Team



# Domain Enumeration Techniques

**Active Directory Module in PowerShell**

**Active Directory Service Interface (ADSI)**

**Open source PowerShell offensive frameworks**



# Information of Interest

**Domain users and  
groups**

**Domain computers**

**Group policies**

**Certificates**

**Service accounts**

**Kerberos  
vulnerabilities**



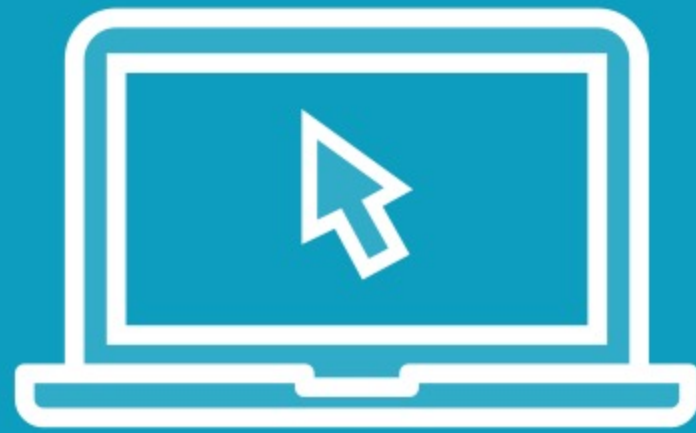
# Demo



## Installing the PowerShell Active Directory module



# Demo



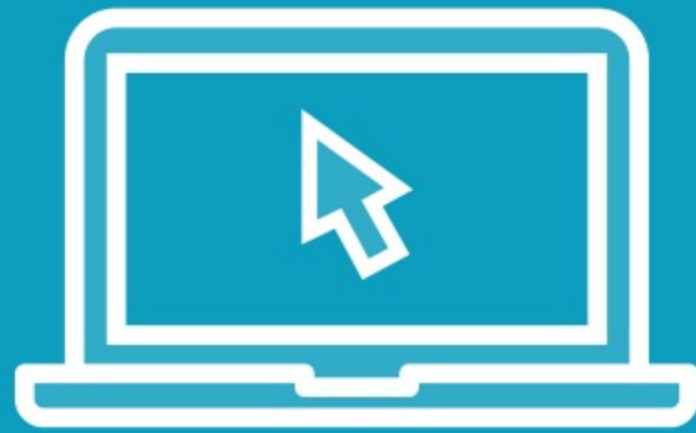
## Enumerating domain users, computers and assets

- Manual enumeration
- Create automated script





# Demo

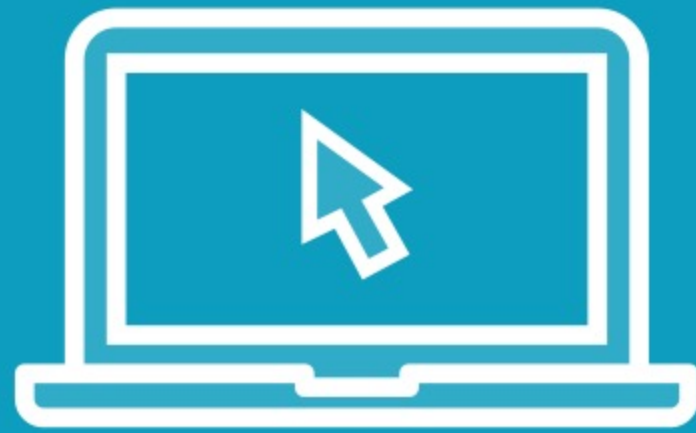


## **Interacting with Active Directory via Active Directory Service Interface (ADSI)**

- Finding information about user accounts



# Demo



## Using an open source tool for Kerberoasting

- Using PowerSploit to retrieve password hashes  
(<https://github.com/PowerShellMafia/PowerSploit>)
- Cracking the hashes and obtaining clear text passwords



# Summary



**Main techniques for active directory enumeration**

**Types of information of interest**

**Enumerating domain information using AD module and ADSI**

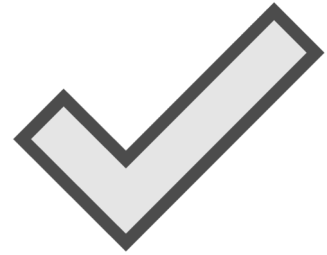
**Executing a Kerberoasting attack and gaining admin privileges**

# Course Closure

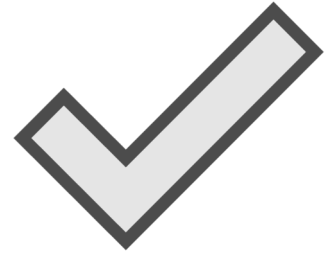
---



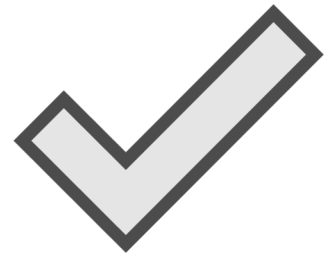
# What You Learned



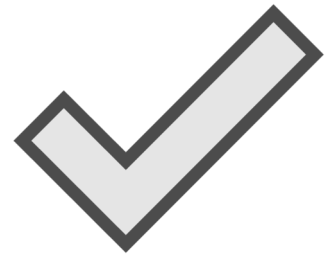
**How PowerShell can help you on a red team engagement**



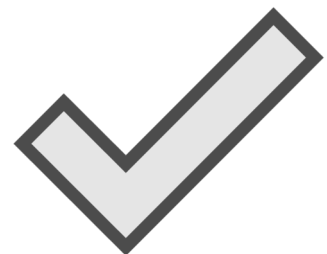
**How to enumerate host information with PowerShell**



**How to scan networks to find live hosts and open ports**



**How to extract information from Active Directory**



**How to use PowerShell open source libraries for offensive security**



# How To Get the Most Out of This Course

**Practice the skills  
you learned**

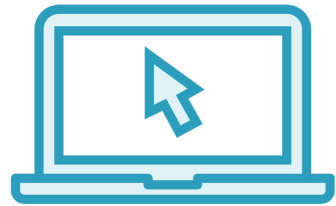
**Code your own tools**

**Review open source  
PowerShell tools**

**Try exploiting different domains  
and OS versions**



# What's Next



## **Other PowerShell courses**

Course Path: PowerShell for Cyber Offense



## **Practice on live environments**

[hackthebox.eu](https://hackthebox.eu) | [pentestit.ru](https://pentestit.ru)



## **Red team tools courses at Pluralsight**

[pluralsight.com/paths/skill/red-team-tools](https://pluralsight.com/paths/skill/red-team-tools)



## **Open source PowerShell offensive frameworks**

Several PowerSploit courses



# Thank you!



**Ricardo Reimao, OSCP, CISSP**  
Cybersecurity Consultant

