

# Network Discovery and Enumeration with PowerShell

---

## Enumerating Local Host Information



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

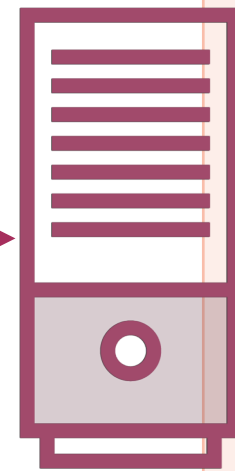


# Leveraging PowerShell for Discovery



# Course Scenario: Globomantics Red Team

Globomantics Network

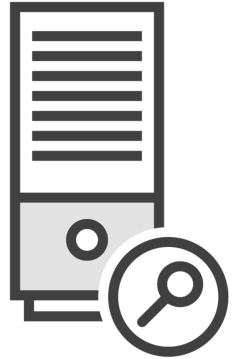


To-Do:

- 1) Enumerate host
- 2) Enumerate network
- 3) Enumerate domain

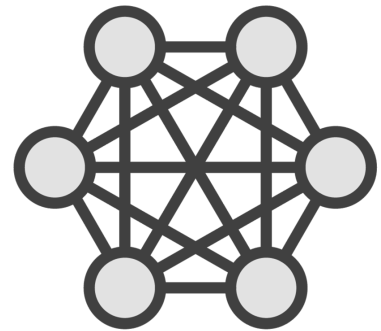


# Course Overview



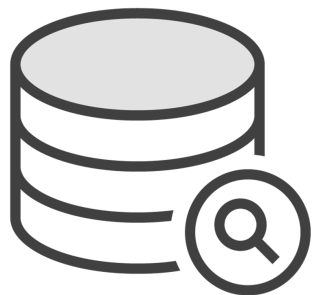
## **Enumerating local host information**

Installed software, patches, users, security products, etc.



## **Enumerating the network**

Finding active hosts, open ports, SMB shares, etc.

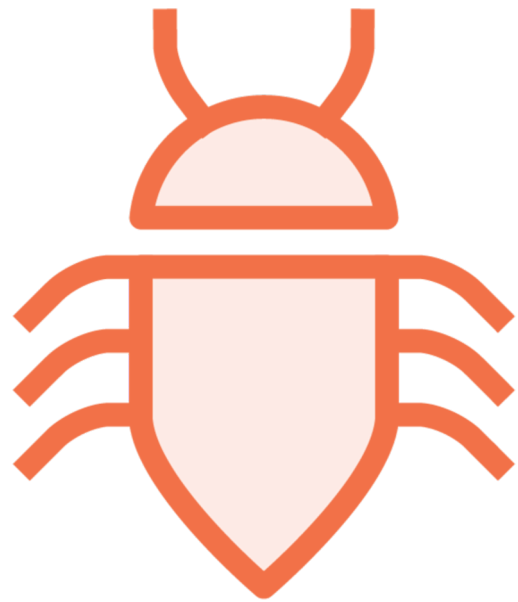


## **Enumerating the domain**

Domain users, computers, service accounts, kerberoasting, etc.



# Recommended Knowledge



**Main security concepts  
and vulnerabilities**



**Basic PowerShell  
knowledge**



**Recommended course path:**  
“Windows PowerShell: Essentials”



# Why Using PowerShell for Red Teaming?

Increased control

Tailored input and output

Avoiding detection



# Collecting Information From Local Hosts

---



# Types of Data of Interest

**Operational system  
information**

**Local users and  
groups**

**Running scripts**

**Logon and RDP  
events**

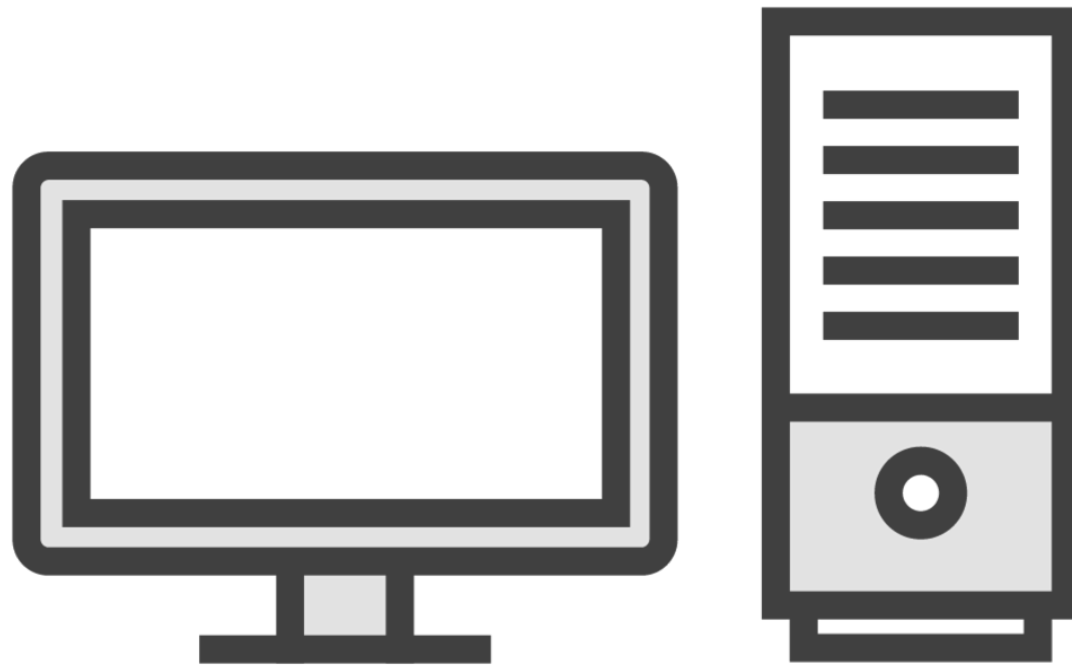
**Installed software**

**Security products**



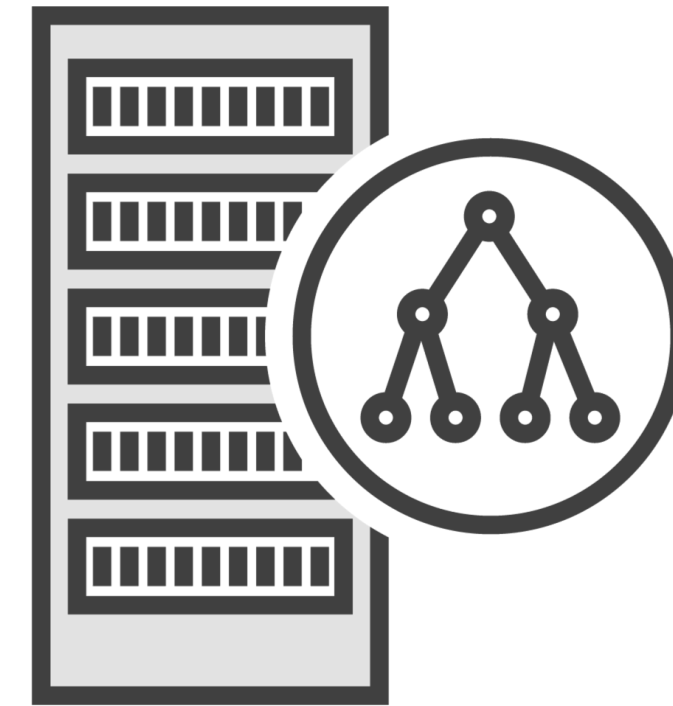


# Lab Environment



**Victim Machine**

Windows Server 2019



**Domain Controller**

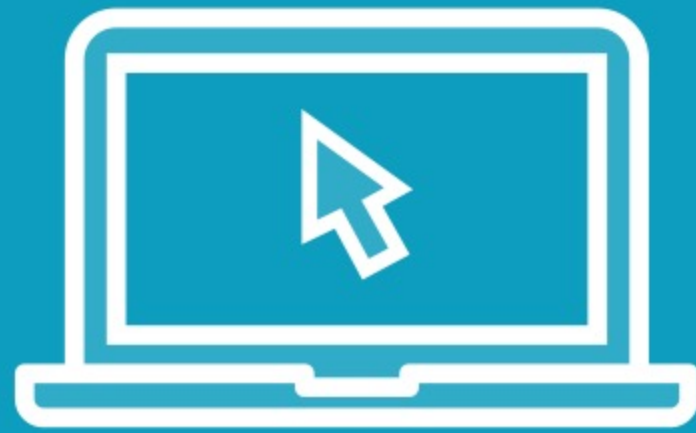
+

**Additional Servers (Optional)**

Windows Server 2016/2019



# Demo

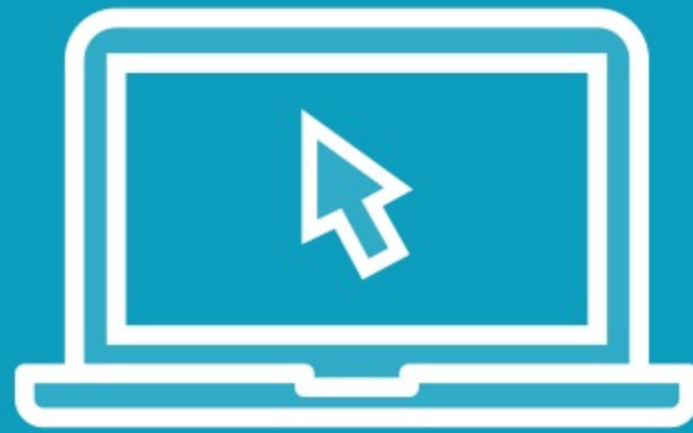


## Local host enumeration

- OS version, patching levels, local users, and much more



# Demo



**Running host enumeration techniques  
in remote systems**



# Demo



**Enumerating software**

**Enumerating security products**



# Demo



## **Automating local host enumeration**

- Merging all commands into one script



# Summary



**Why using PowerShell in offensive security**

**How to enumerate host information and installed software**

**Creating an automated host information enumeration script**



**Next up:**  
Enumerating Network Hosts

