

Privilege Escalation with Rubeus



Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant



Why Escalating Privileges?



Rubeu
s



Rubeus

Primary Author: Harmj0y (@harmj0y)

A tool for raw Kerberos interaction and abuses.



Rubeus

Open source software

<https://github.com/GhostPack/Rubeus>

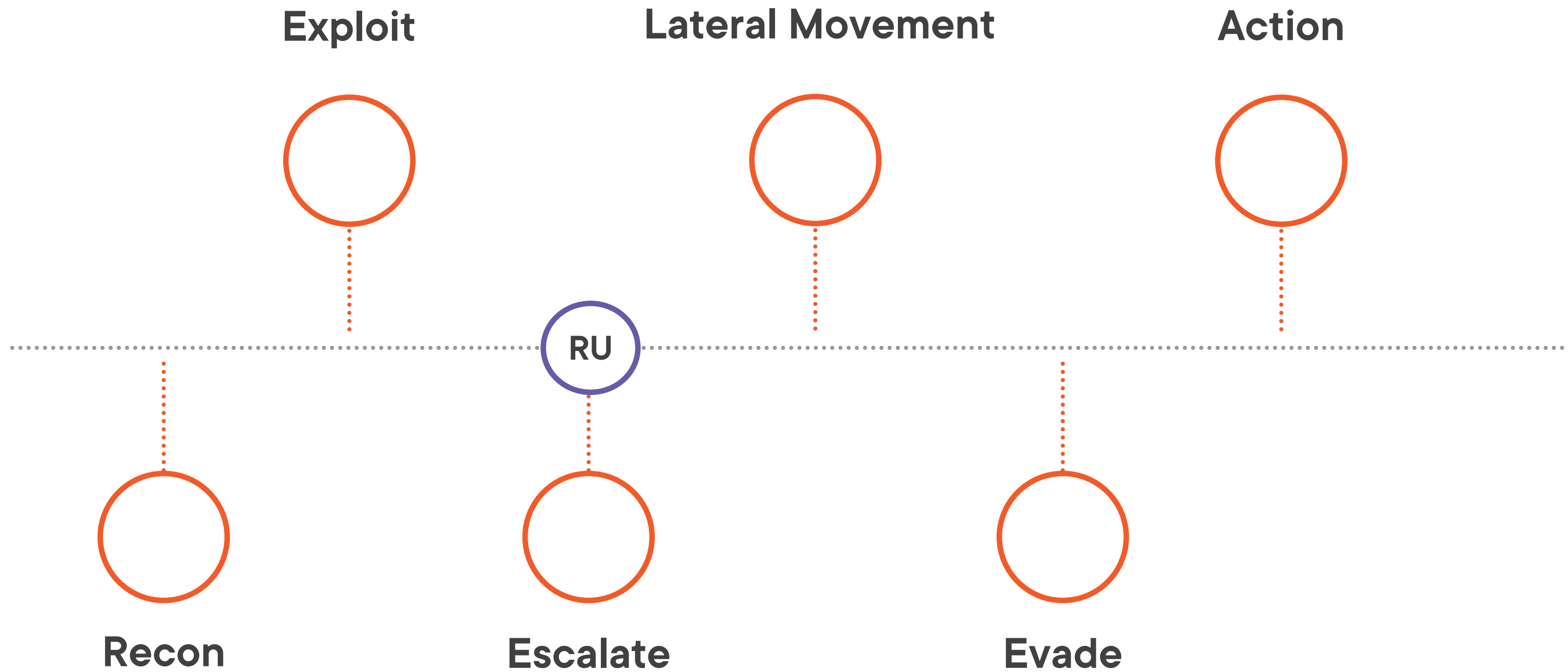
Facilitate the interaction with Kerberos

Automates several privilege escalation attacks

- Kerberoasting
- AS-REP Roasting
- Pass the Hash / Pass the Ticket
- Golden Ticket
- Silver Ticket



Kill Chain



MITRE ATT&CK

Tactics

Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact



MITRE ATT&CK

Tactics

Reconnaissance

Resource Development

Initial Access

Execution

Persistence

Privilege Escalation

T1134:

Access Token Manipulation

Defense Evasion

Credential Access

T1558:

Steal or Forge Kerberos Tickets

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1558.003:

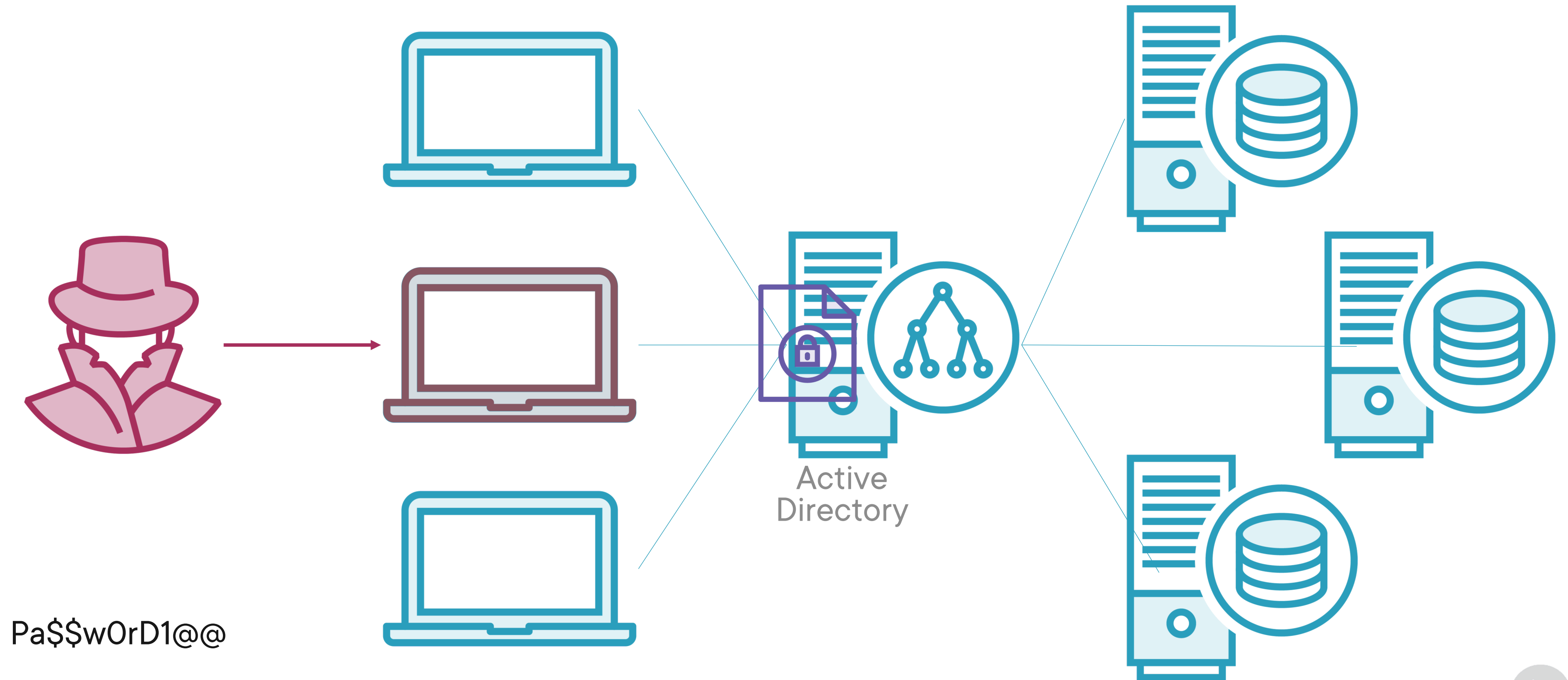
Kerberoasting

T1558.004:

AS-REP Roasting



Lab Explanation

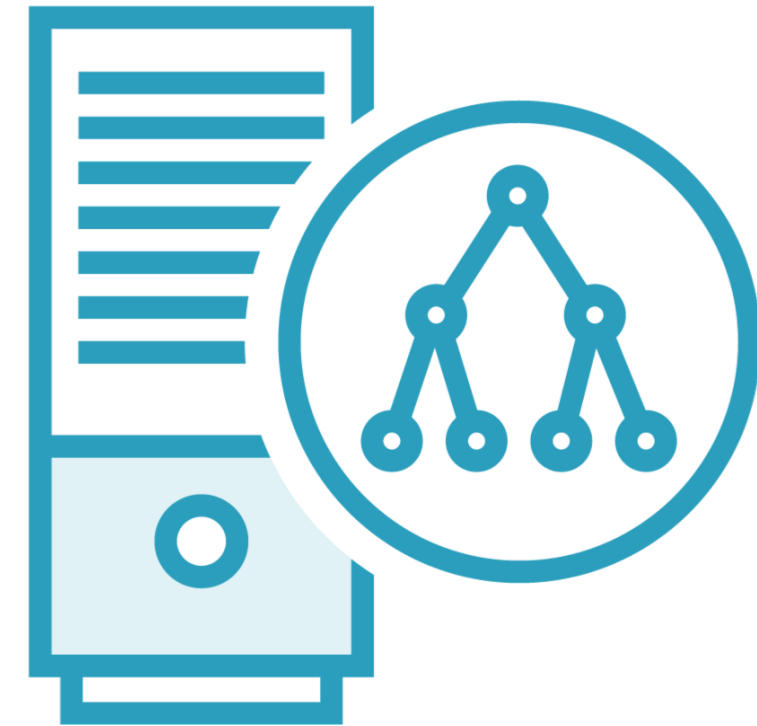


Prerequisites



User Laptop

Windows integrated with the
Active Directory



Active Directory

Windows Server 2016
with service accounts



Demo Place Holder

1. Installation Tips and Tricks
2. First use instructions and common usage syntax
3. Use of main features on live targets or in live environment



Demo 2 Place Holder

1. Installation Tips and Tricks
2. First use instructions and common usage syntax
3. Use of main features on live targets or in live environment



More Information

Official Documentation

Several other capabilities

<https://github.com/GhostPack/Rubeus>

Other Features

Silver Ticket Attack

Golden Ticket Attack

Recommended Courses

“Credential Access with Responder”

“Post Exploitation with Meterpreter”

Remediation

Adopt strong passwords for service accounts

Password management tool

Use secure configurations



Thank you!



Ricardo Reimao
Cyber security consultant

