Credential Access with THC Hydra

PASSWORD CRACKING WITH THC HYDRA

Lee Allen
PENETRATION TESTER

www.securitysession.com

THC HYDRA
Creator: van Houser/THC

Used towards brute forcing of network logins.
Powerful and fast parallel password cracking tool
with a wide variety of supported network protocols.

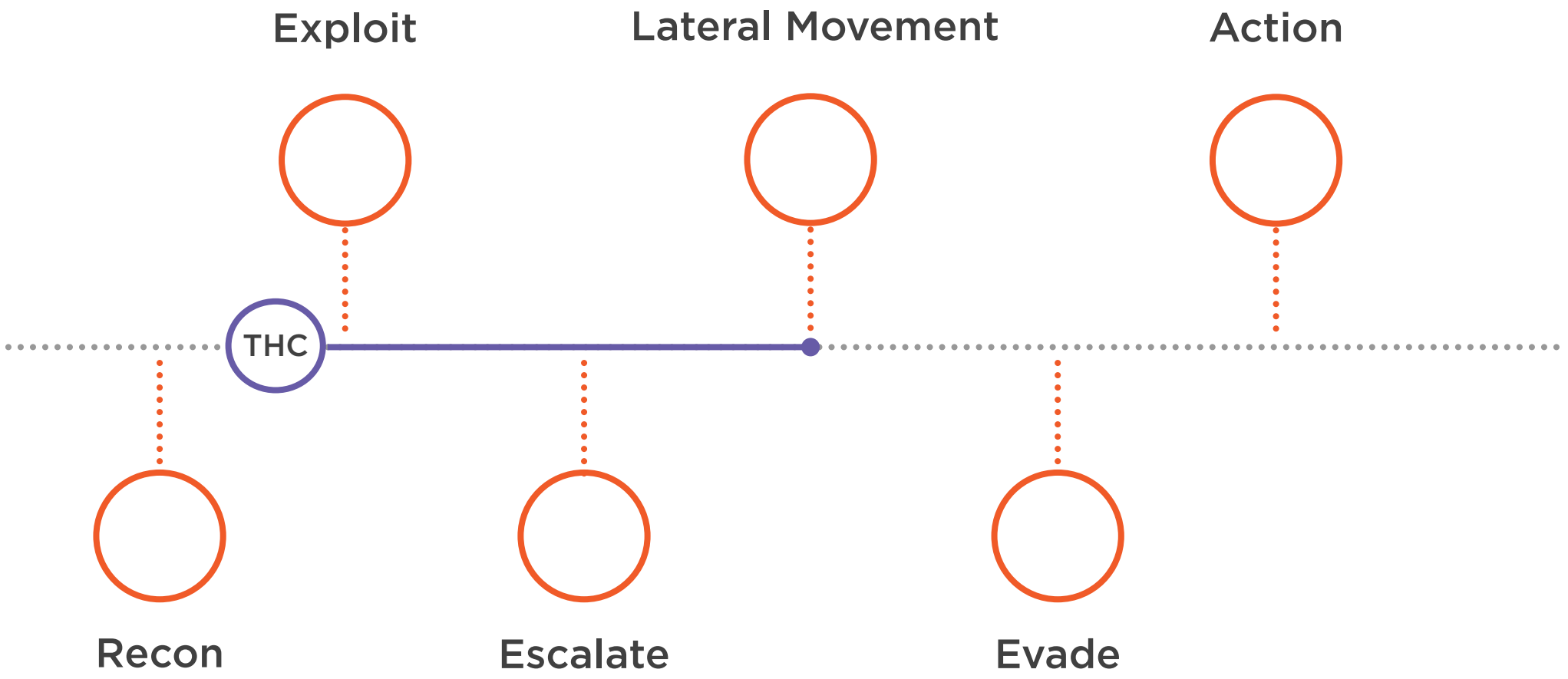
THC Hydra

Available at github.com/vanhauser-thc/thc-hydra for download and compilation

Support for most major platforms including macOS, Windows/Cygwin, Solaris, FreeBSD, and Linux

Preinstalled on Kali Linux 2019

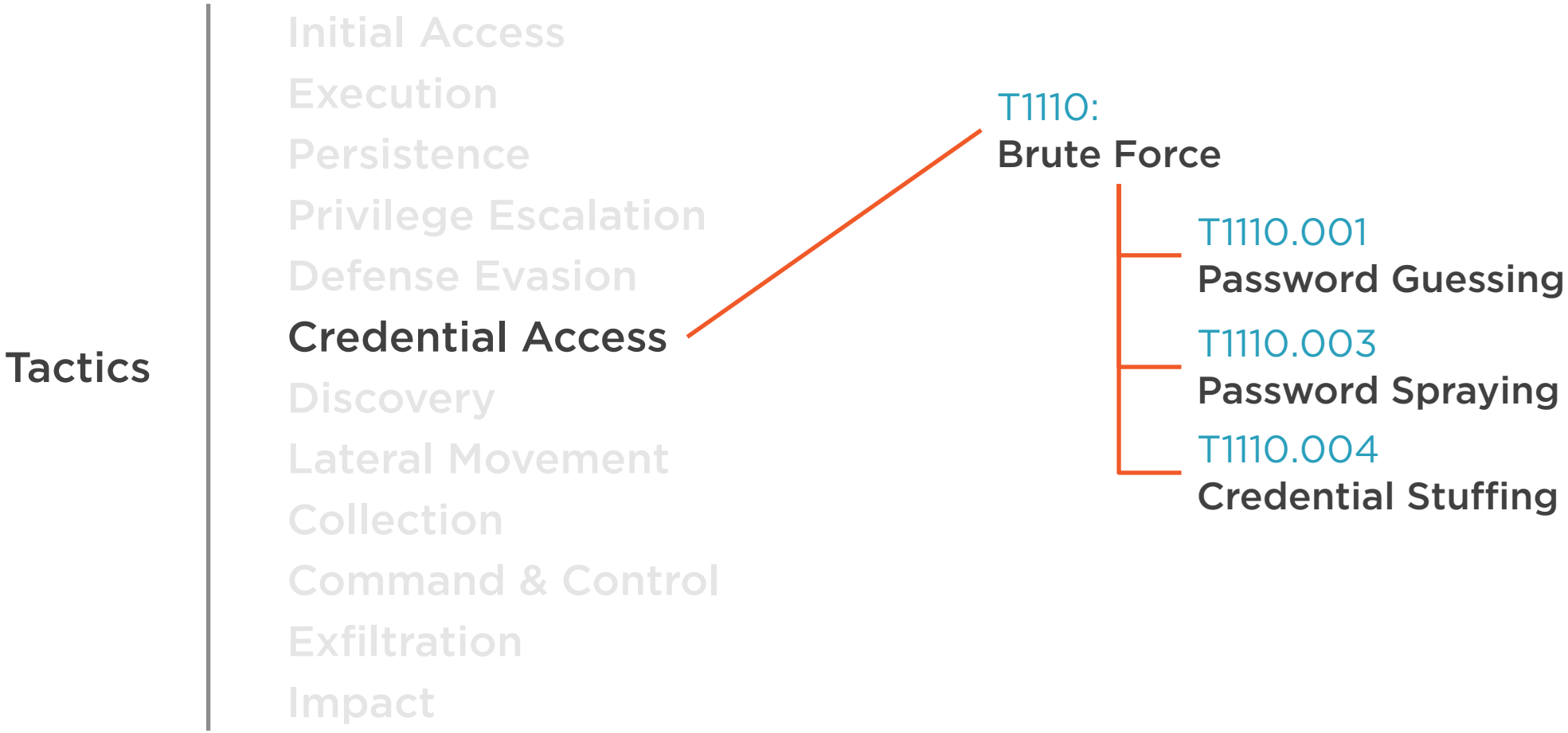
Kill Chain

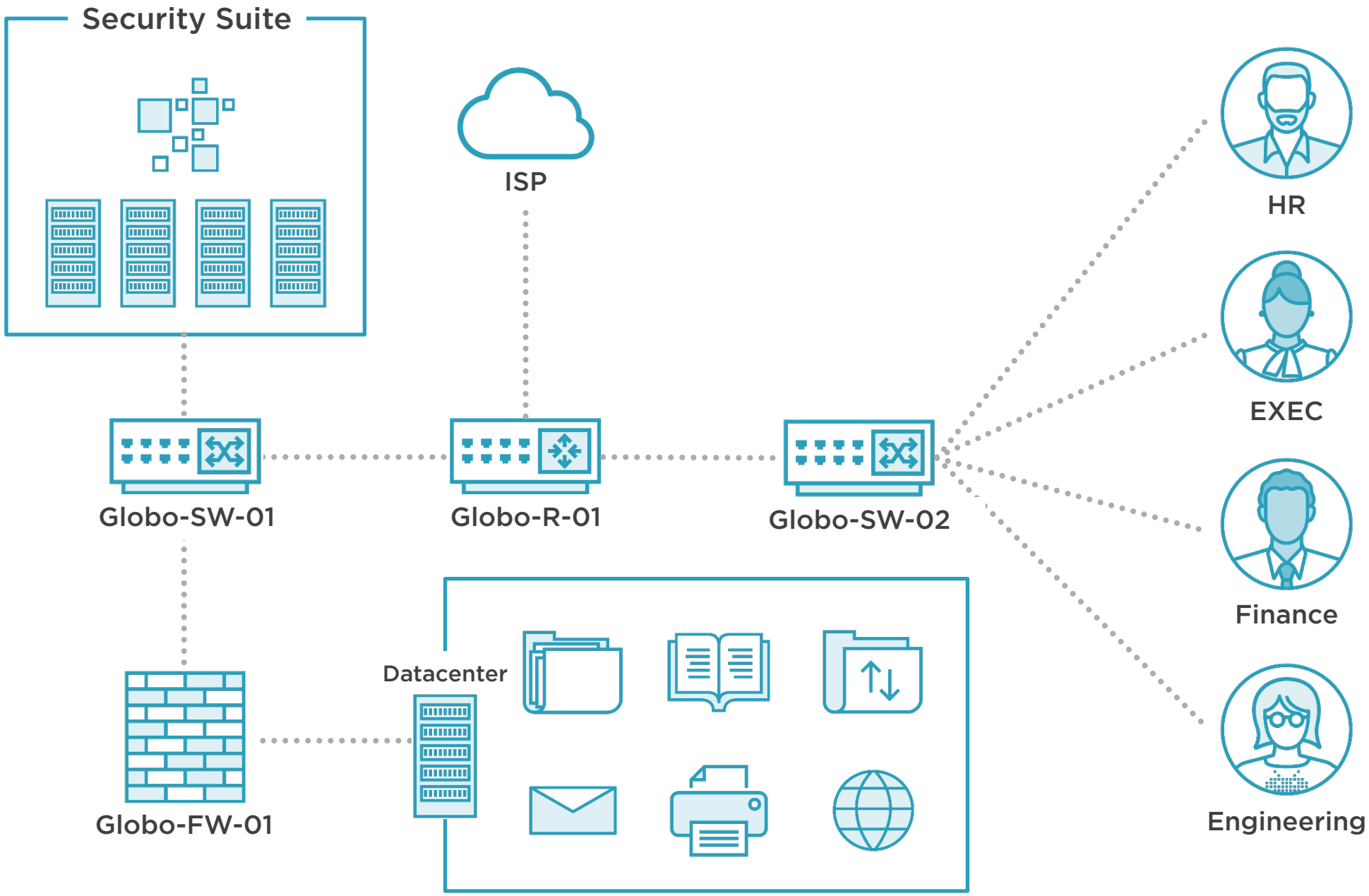


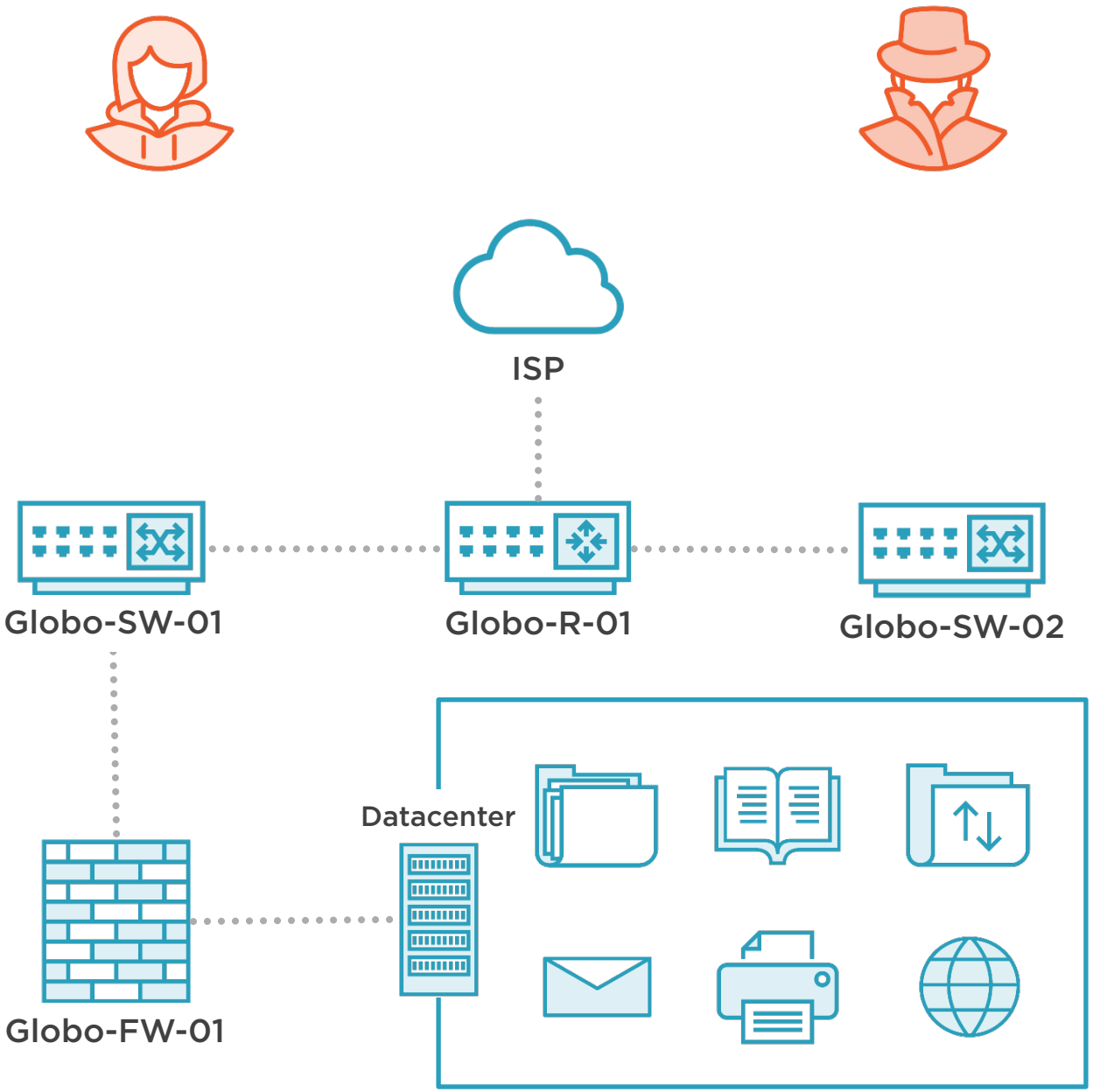
MITRE ATT&CK

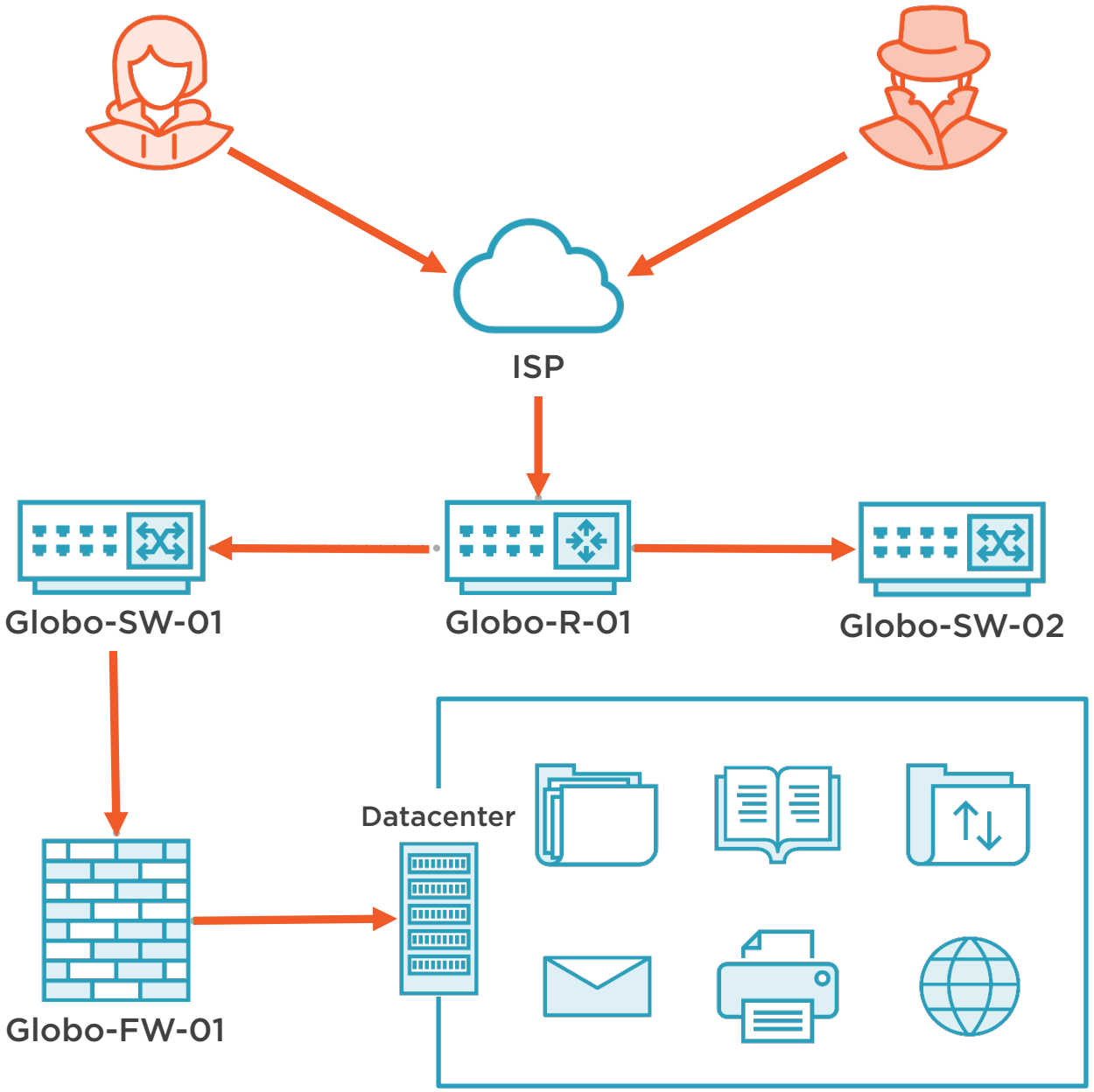
Tactics	Initial Access Execution Persistence Privilege Escalation Defense Evasion Credential Access Discovery Lateral Movement Collection Command & Control Exfiltration Impact

MITRE ATT&CK

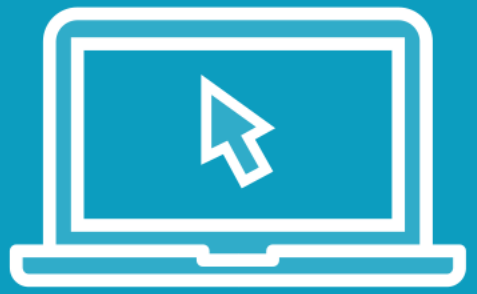

Tactics
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact
T1110:
Brute Force
T1110.001
Password Guessing
T1110.003
Password Spraying
T1110.004
Credential Stuffing


Security Suite
ISP
HR
EXEC
Finance
Engineering
Globo-SW-01
Globo-R-01
Globo-SW-02
Globo-FW-01
Datacenter


ISP
Globo-SW-01
Globo-R-01
Globo-SW-02
Datacenter
Globo-FW-01

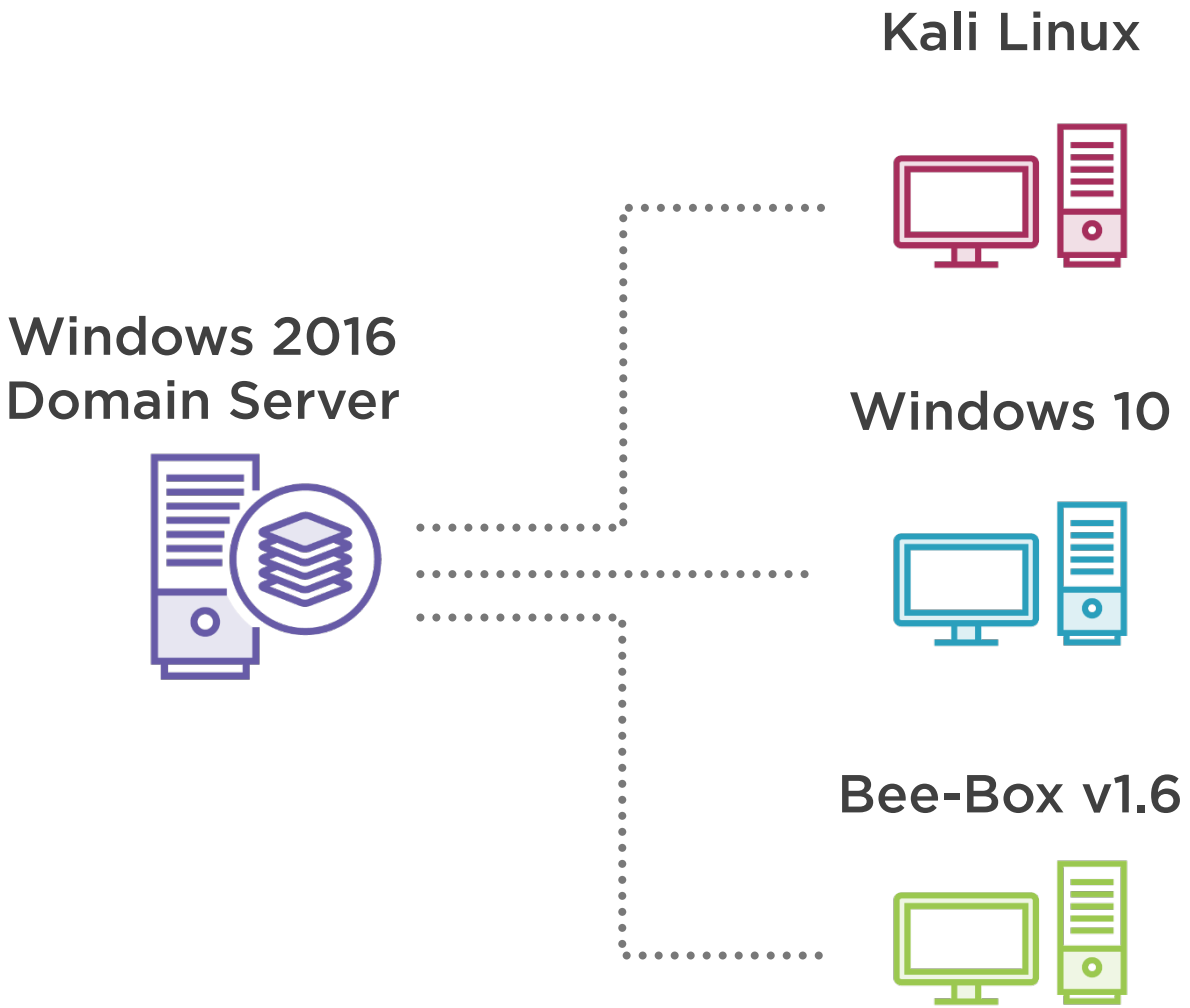

ISP
Globo-SW-01
Globo-R-01
Globo-SW-02
Datacenter
Globo-FW-01

Demo



- Basics of hydra
- Brute force a website login
- Combining a list of usernames with a list of passwords
- Resuming an interrupted session
- Looping passwords around users
- Targeting RDP
- Using a proxy
- Leveraging debug to identify problems

Globomantics Demo Lab



Important Files

Usernames

Text file containing a listing of usernames pulled from Active Directory

Passwords

Short listing of passwords that are preferably targeted at the environment being tested.

More Information

"I have not failed. I've just found 10,000 ways that won't work." -Thomas Edison

Popular Word Lists

Probable Wordlists

github.com/berzerk0/Probable-Wordlists

SecLists

github.com/danielmiessler/SecLists

Word List Generators

Common User Passwords Profiler

github.com/Mebus/cupp

CeWL Custom Word List Generator

github.com/digininja/CeWL