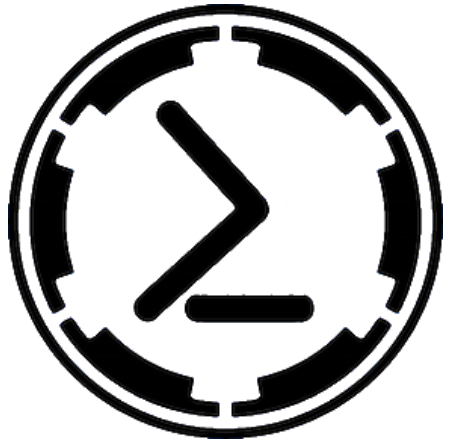
Command and Control with Empire

Rishalin Pillay

OFFENSIVE CYBER SECURITY AUTHOR & SPECIALIST

@r1shal1n



PowerShell Empire (PSEmpire) Creator: @harmjoy, @sixdub, @enigma0x3, rvrsh3ll, @killswitch_gui & @xorrior.
https://github.com/EmpireProject/Empire/

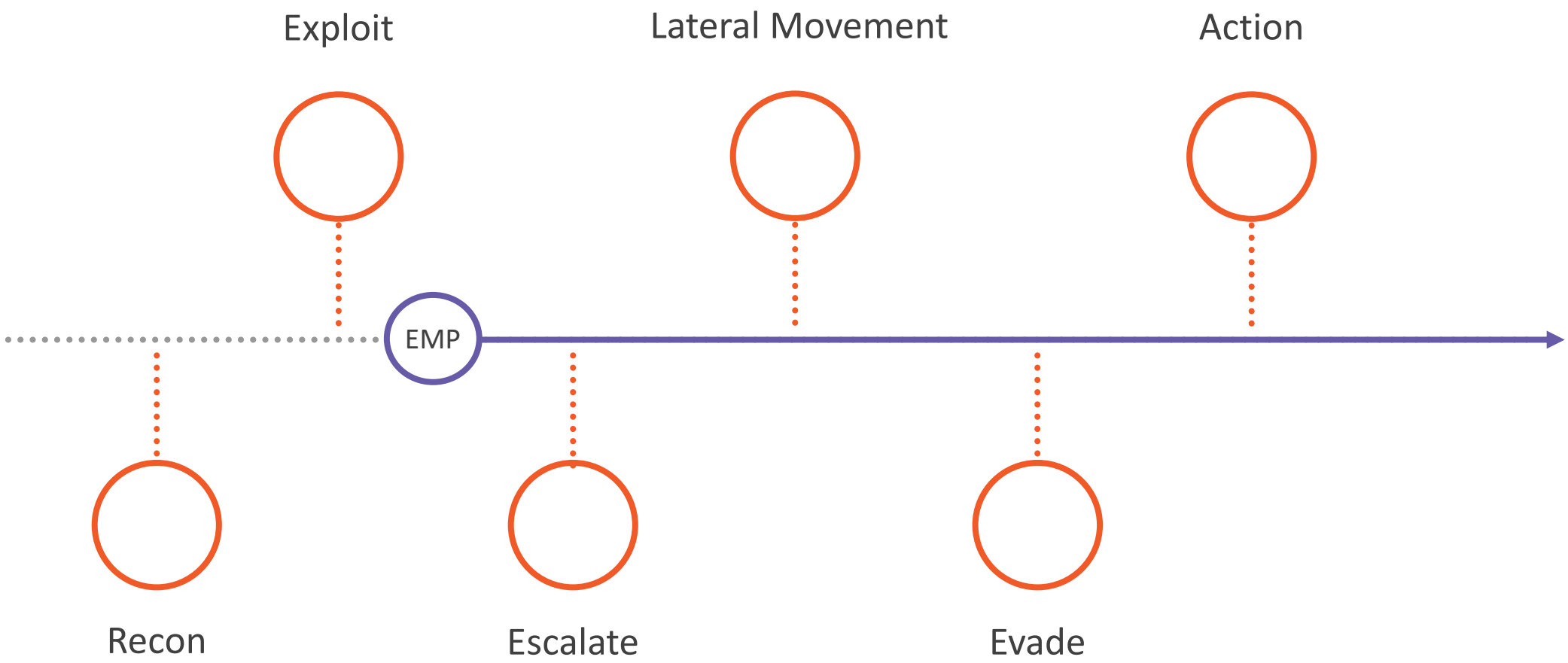
Empire : Maintained by BC-Security
https://github.com/BC-SECURITY/Empire/

Empire 3 is a pure PowerShell post exploitation framework. It merged the previous PowerShell Empire and Python EmPyre projects.

Starkiller Creator: BC-Security
https://github.com/BC-SECURITY/Starkiller/

Multi-user GUI for interfacing with the Empire server.

Kill Chain



MITRE ATT&CK

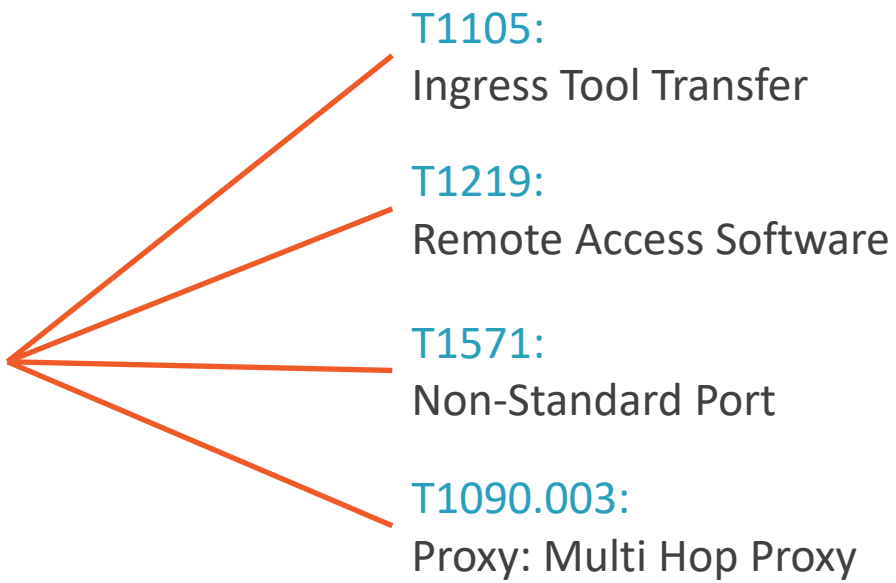
Tactics

- 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



Kali Linux 2020.3

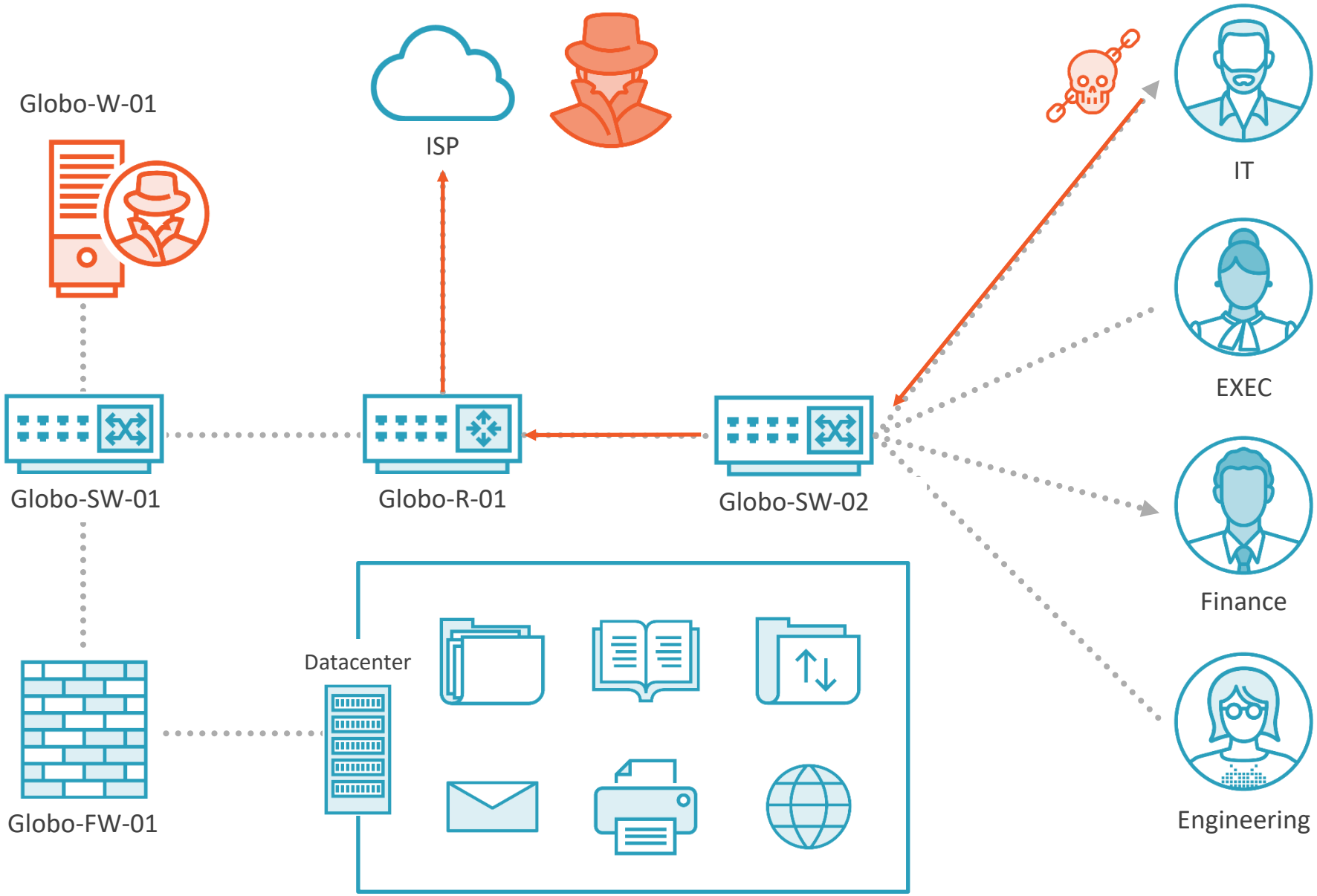
Up to date:

apt-get update

apt-get upgrade

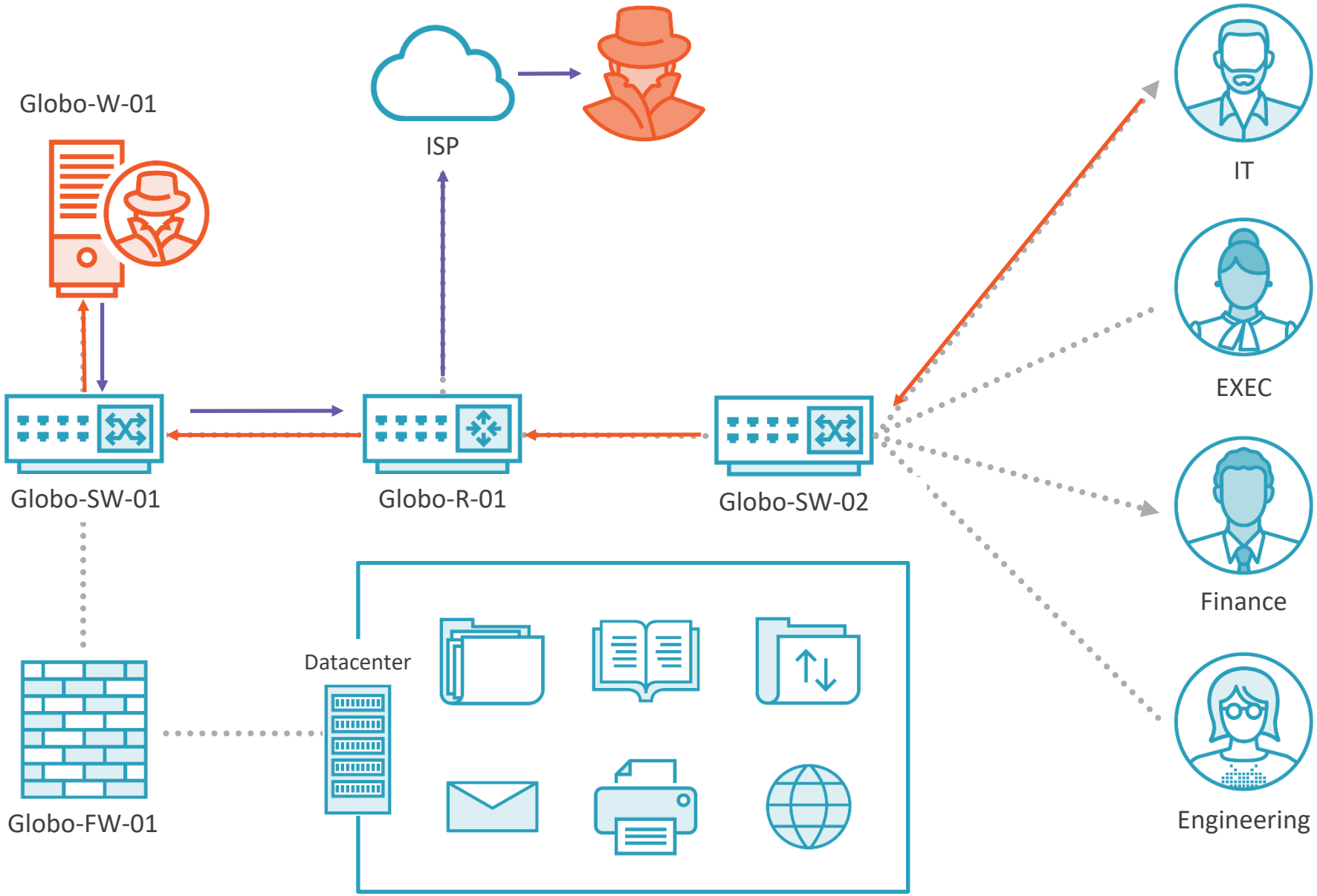
Empire Workflow

- Listeners
- Stagers
- Agents
- Modules


Globo-W-01
ISP
IT
EXEC
Finance
Engineering
Globo-SW-01
Globo-R-01
Globo-SW-02
Datacenter
Globo-FW-01

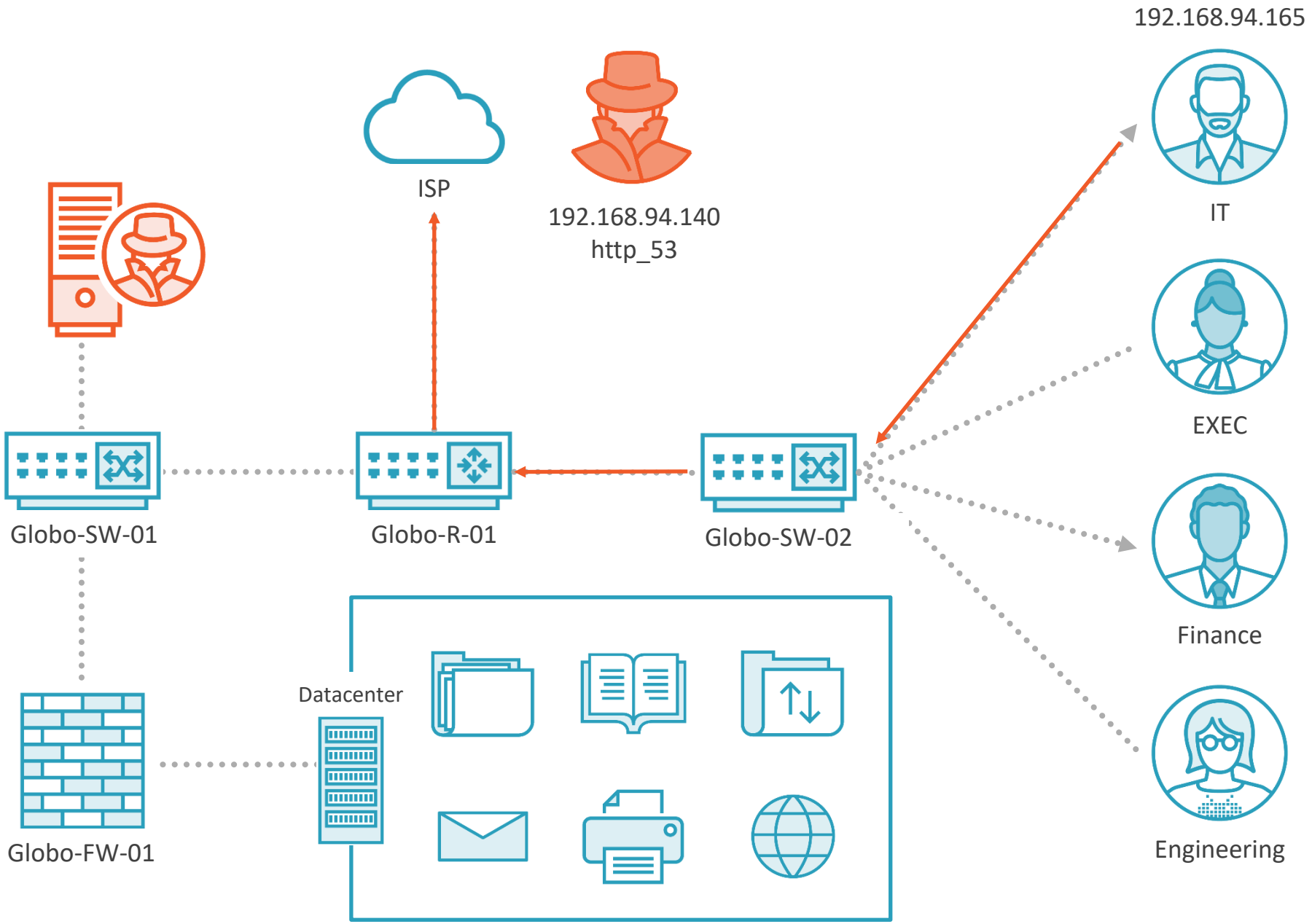
Demo

Proxying traffic using http_hop


Globo-W-01
ISP
IT
EXEC
Finance
Engineering
Globo-SW-01
Globo-R-01
Globo-SW-02
Datacenter
Globo-FW-01

Demo

Non-standard port


192.168.94.165
ISP
192.168.94.140
http_53
IT
EXEC
Finance
Engineering
Globo-SW-01
Globo-R-01
Globo-SW-02
Globo-FW-01
Datacenter

Demo

Enable RDP for C2

Upload files

More Information

Documentation

Empire Documentation

https://www.powershellempire.com/

Related Information

Persistence with Empire – Pluralsight

MITRE ATT&CK Software Page

- https://attack.mitre.org/software/S0363/

Thank you!

Rishalin Pillay
Cybersecurity Author &
Specialist