Pen Testing Is Broken

Zach Grace
@ztgrace

zach@bsides:~# id

- Lead Security Consultant at a Fortune 100
- Former Manager of Penetration testing at 403 Labs
- Wisconsin CCDC Red Team member
- @MilSec hacker herder

A Better Approach

- Offense - provide more value to defense
- Defense - a different approach to securing your environment

What is Pen Testing?

- Meant to be a simulated attack
- Proves if someone can break in
- Shows the impact once they’re inside

TARGET

J.P.Morgan

THE HOME DEPOT

SC DOR

Anthem

Pen Testing is the new AV

What's Broken With Pen Testing?

- Vulnerability focused
- Reporting doesn't help defenders
- Lack of realistic threat modeling

Vulnerability Focused

- Shutdown a single attack path
- False sense of security

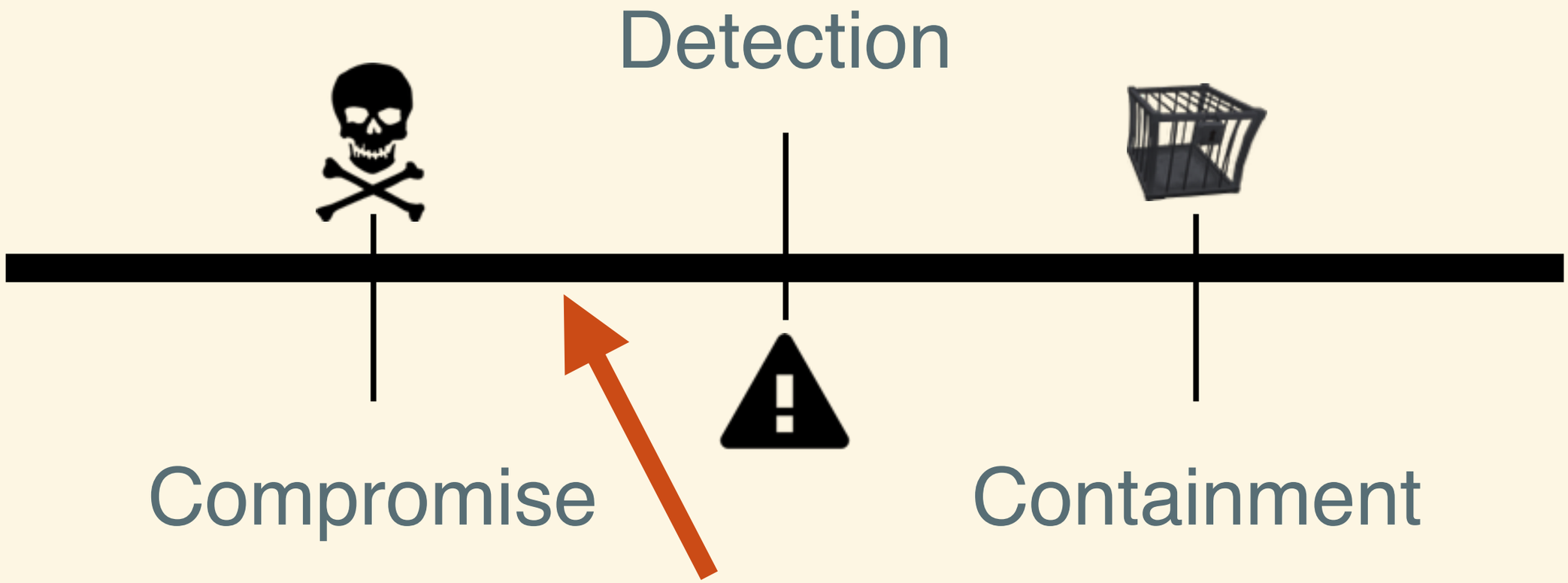
Typical Report

Who Ya Modeling?

```
[04:35:30][root@fry:~]# responder -i eth0
NBT Name Service/LLMNR Responder 2.0.
Please send bugs/comments to: lgaffie@trustwave.com
To kill this script hit CRTL-C

[+]NBT-NS, LLMNR & MDNS responder started
[+]Loading Responder.conf File..
Global Parameters set:
Responder is bound to this interface: ALL
Challenge set: 1122334455667788
WPAD Proxy Server: False
WPAD script loaded:  function FindProxyForURL(url, host){if ((host == "loc
)) return "DIRECT"; return 'PROXY ISAProxySrv:3141; DIRECT';}
HTTP Server: ON
HTTPS Server: ON
SMB Server: ON
SMB LM support: False
Kerberos Server: ON
SQL Server: ON
FTP Server: ON
IMAP Server: ON
POP3 Server: ON
SMTP Server: ON
DNS Server: ON
LDAP Server: ON
FingerPrint hosts: False
Serving Executable via HTTP&WPAD: OFF
Always Serving a Specific File via HTTP&WPAD: OFF
```

It’s not if, but when…


Detection
Compromise
Containment
MTD - MTC = Δ

Δ Force

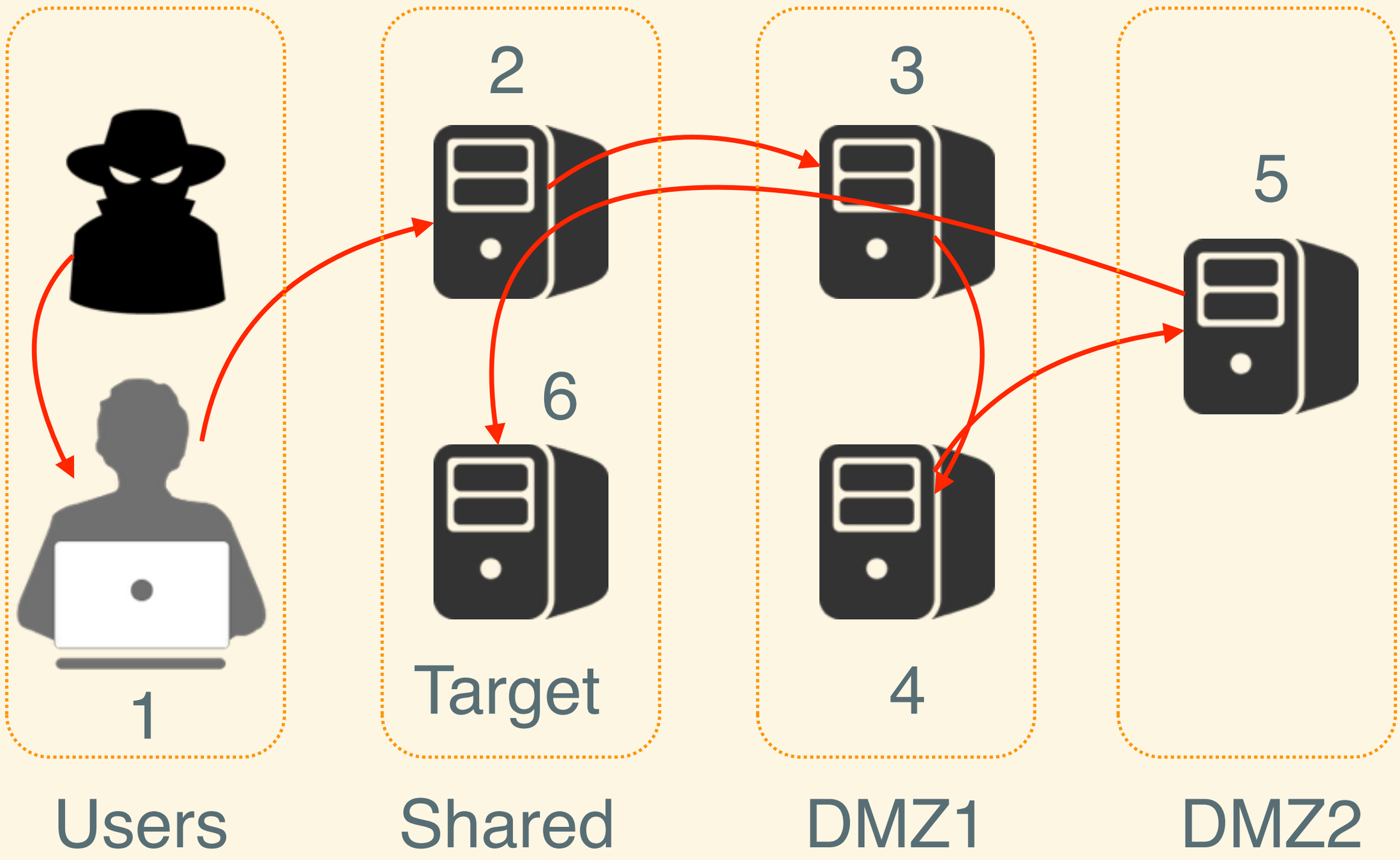
Δ Force Objectives

- Perform threat simulations based on threat modeling
- Breakdown attacks into stages
- Validate detection at each stage, and assist with correlation
- Provide attack use cases besides vulns in reports

Threat Modeling TL;DR

- Who are you?
- What are you going after?

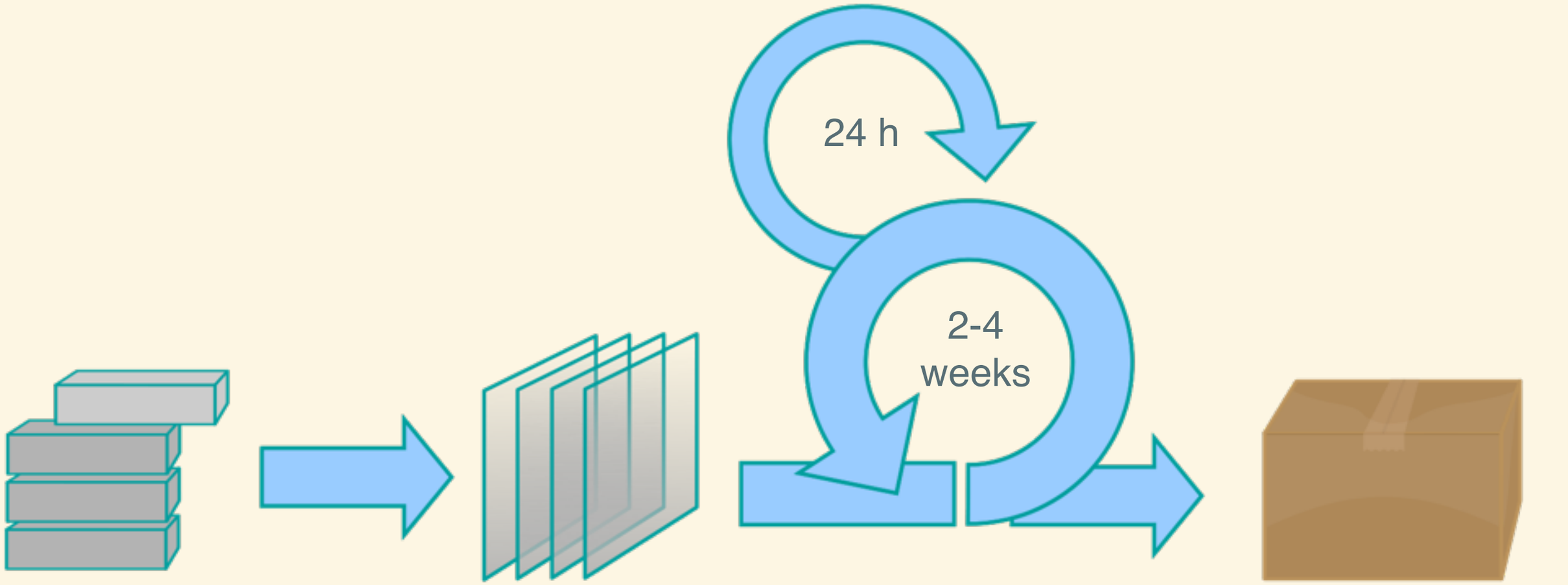
Attack Paths



What About Defense?

- Delivering large capabilities is hard
- Let’s borrow some methodology from agile application development

Scrum Sprint Cycle



http://en.wikipedia.org/wiki/Scrum_(software_development)

Start With A Backlog

Feature	Priority	Size
Exfiltration	1	Small
Malware Detection	2	Medium
Lateral Movement	3	Large
Privilege Escalation	4	X-Large

User Story

As a user

I would like to search for people

so that I can find my friends.

Security User Story

As a defender

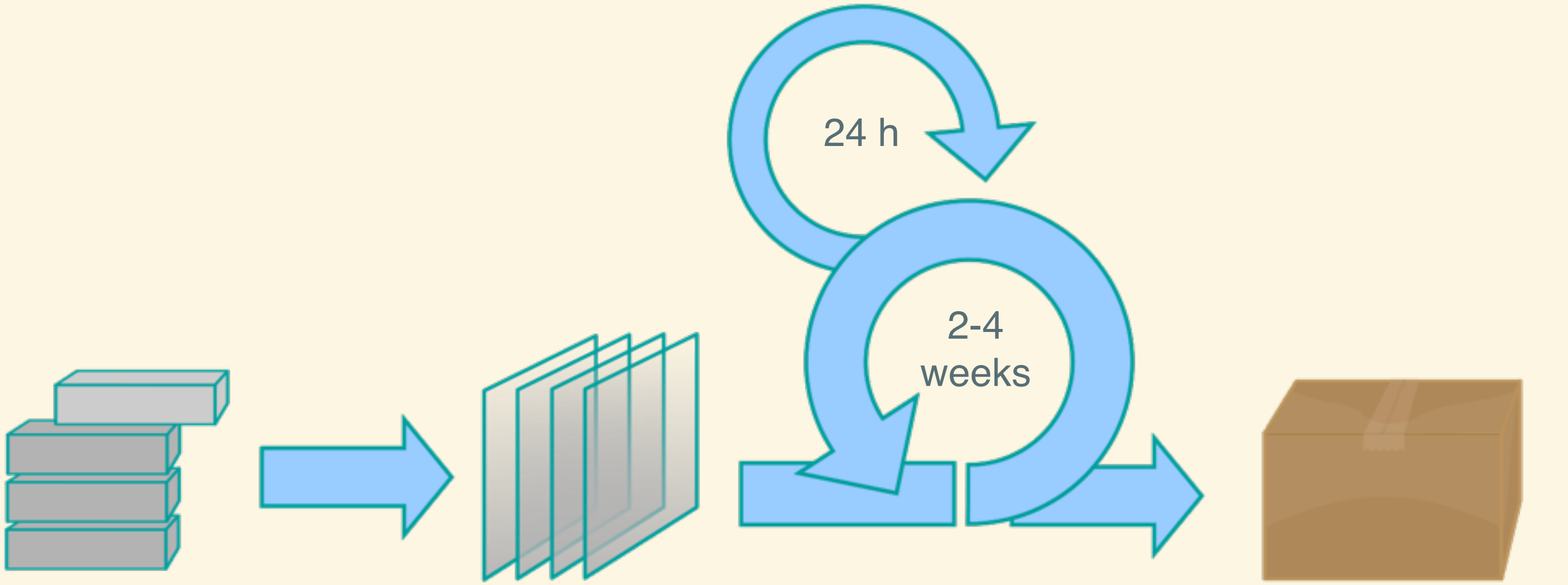
I would like to monitor netflow

so that I can detect lateral movement.

Detailed Backlog

Feature	Sec Story	Task	Size
Lateral Movement	NetFlow	PTH	16 hours
Lateral Movement	NetFlow	Port Scanning	8 hours
Privilege Escalation	HIDS	Mimikatz	1 week
Exfiltration	DLP	> 50MB	2 weeks

Scrum Sprint Cycle



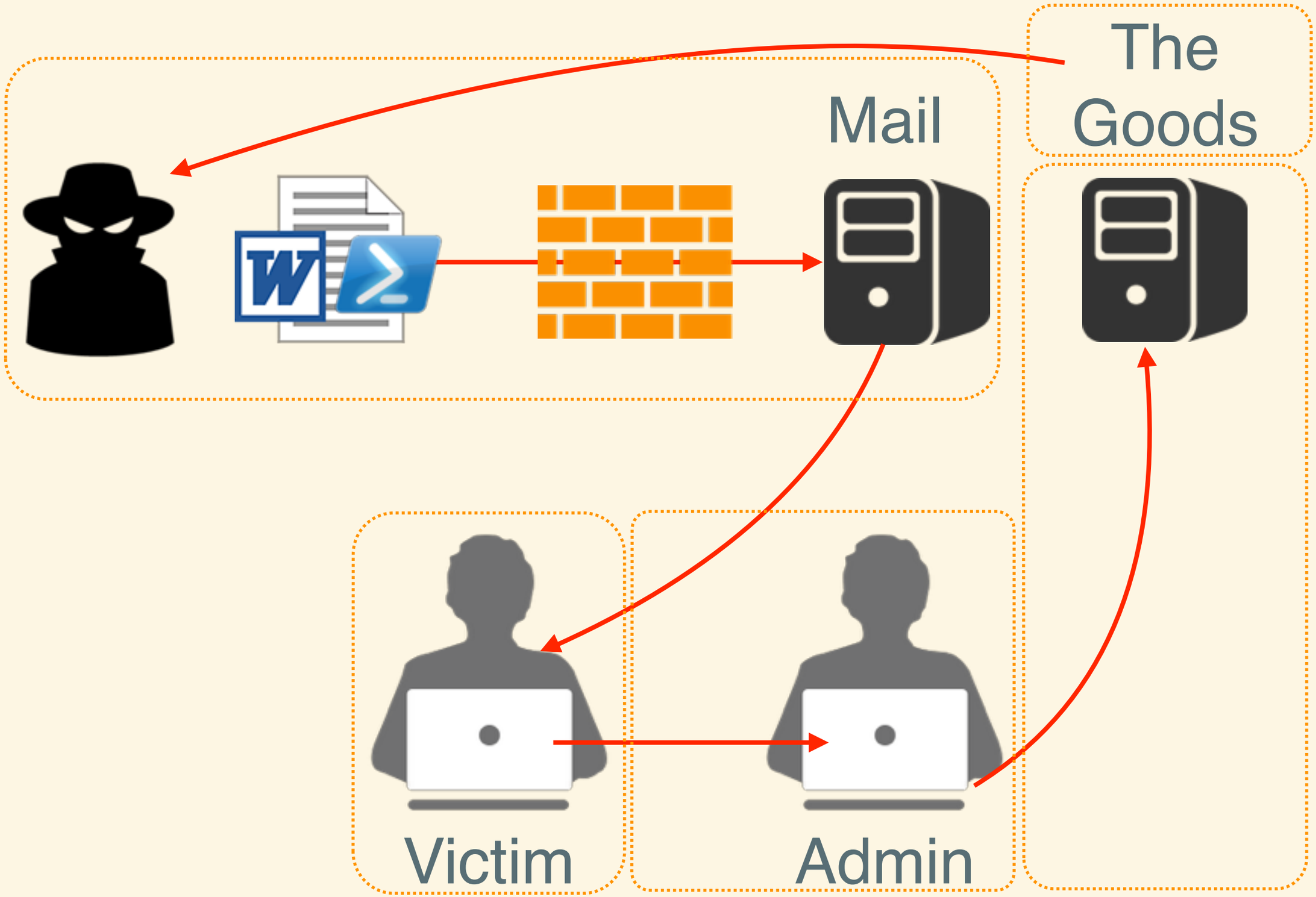
http://en.wikipedia.org/wiki/Scrum_(software_development)

Putting It Together

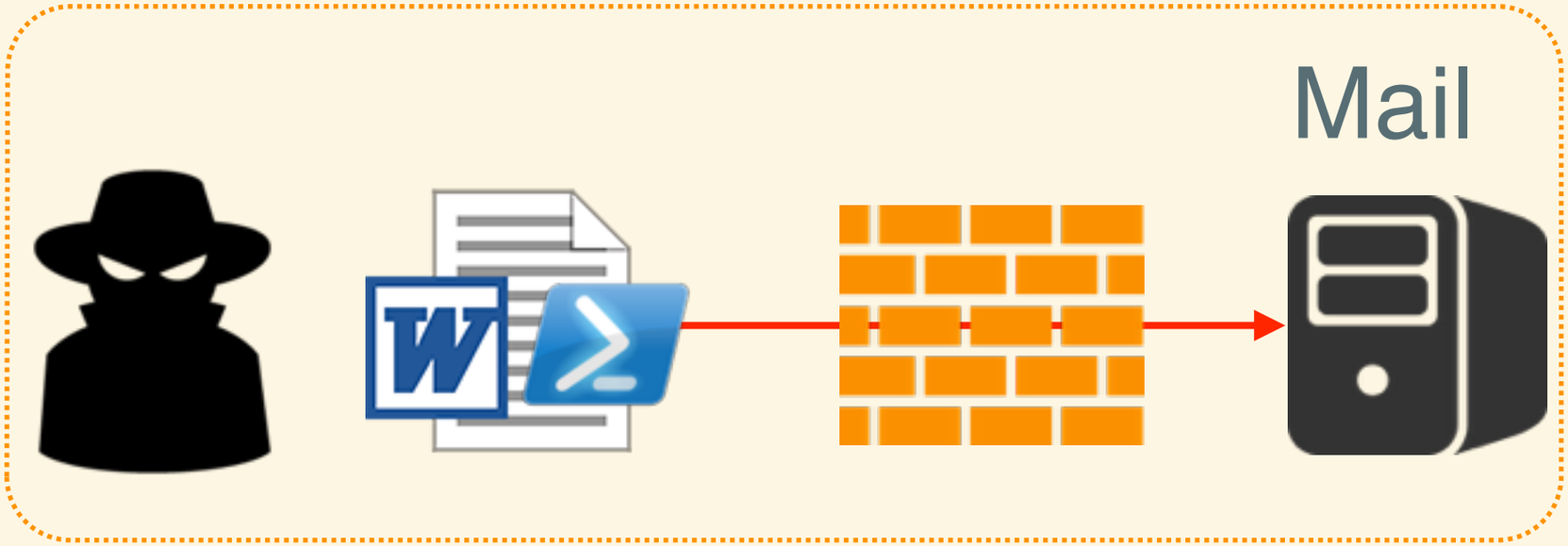
Threat Modeling

Targeted spear-phishing attack from an external actor going after the goods.

Phishin' fo the Goods

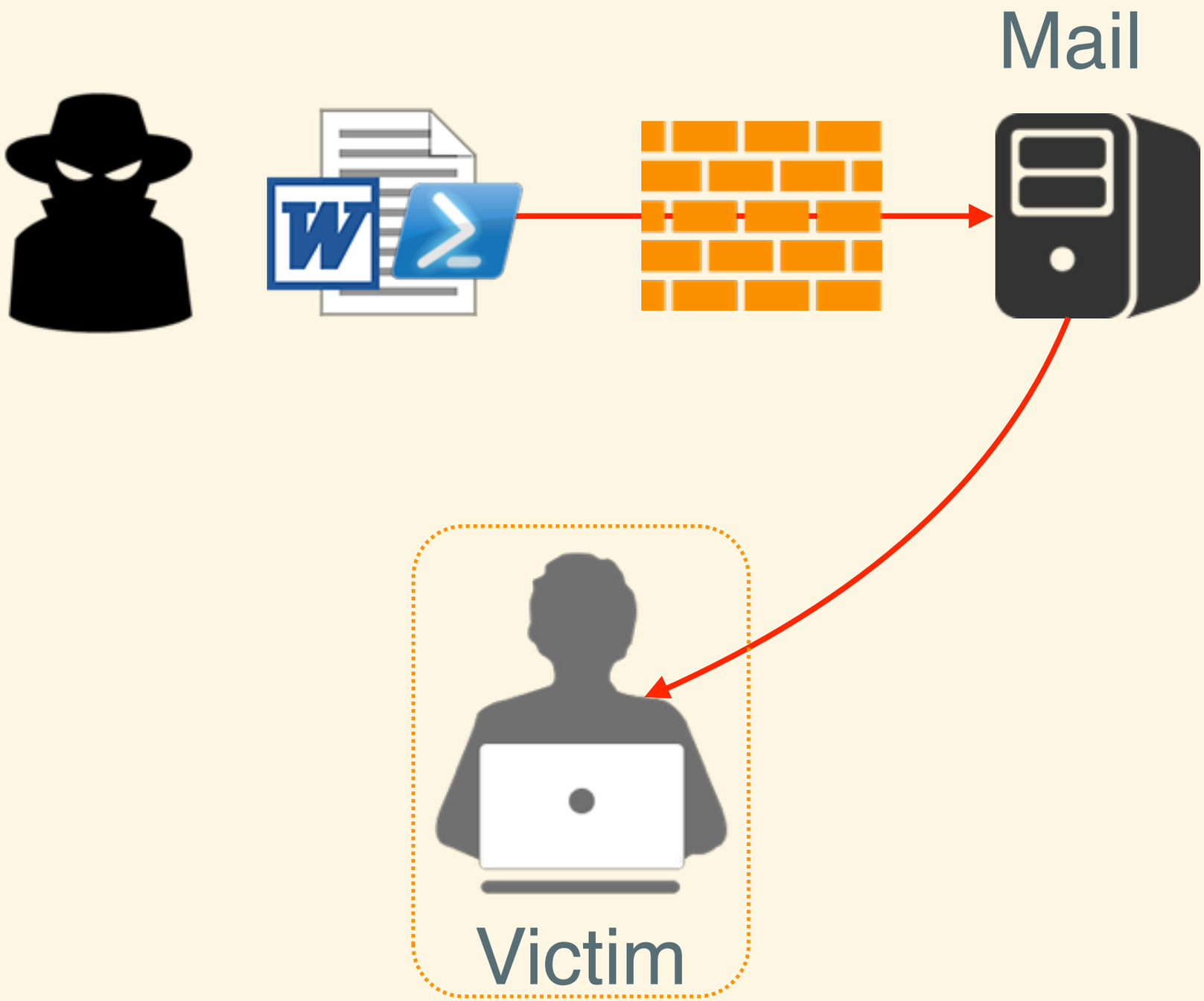


Bypass Mail Controls

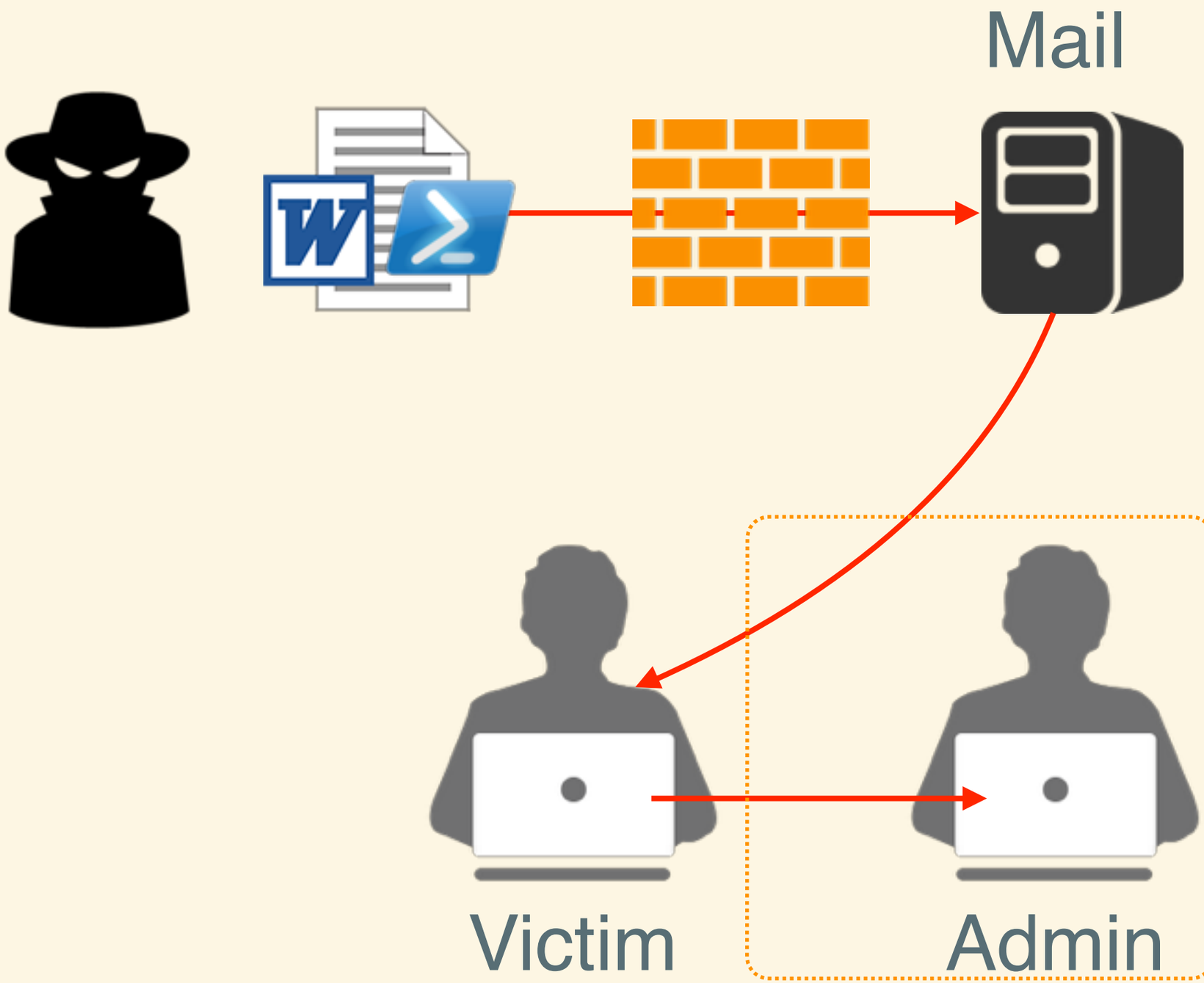


As a defender
I would like to detect and block malicious doc files
so that I can prevent patient zero.

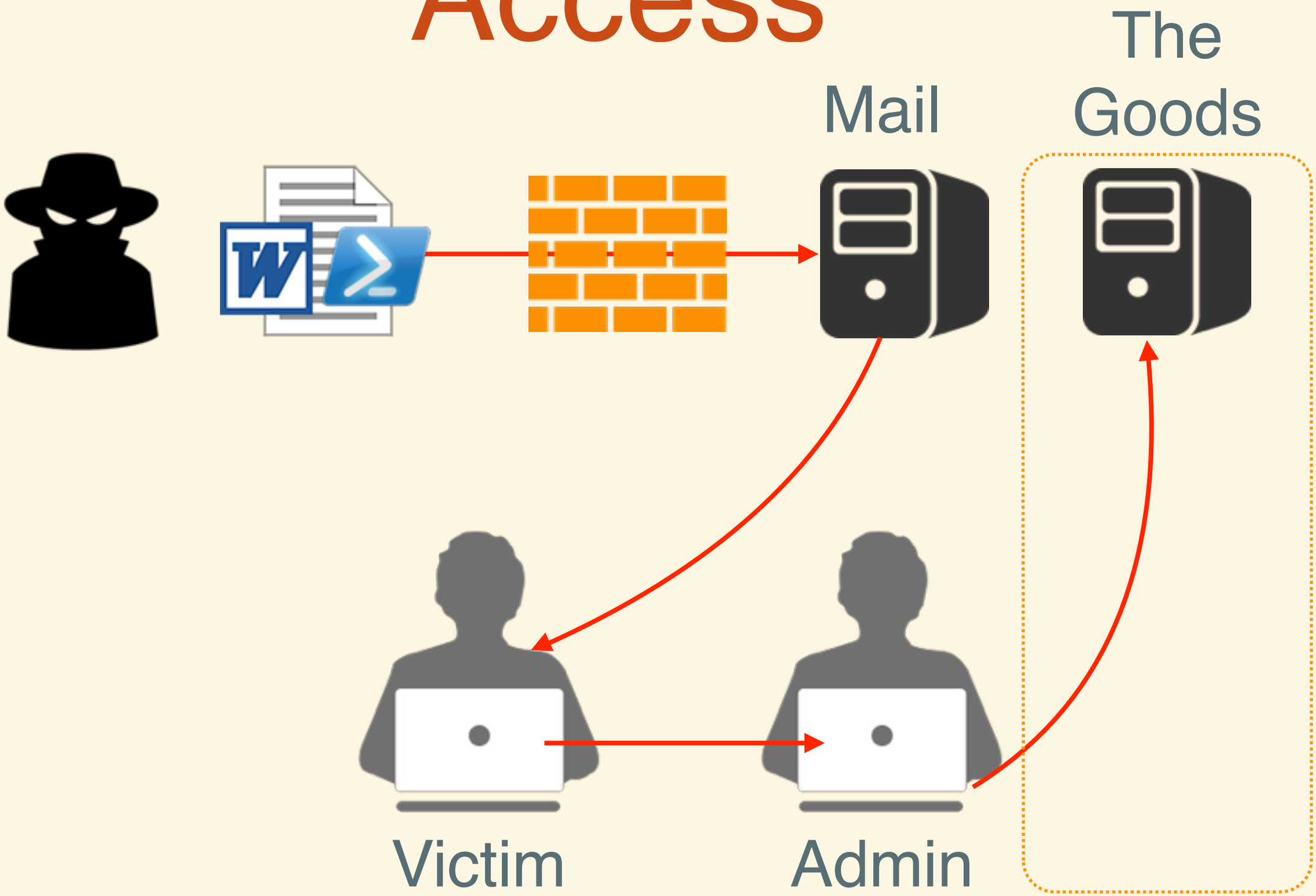
Executing Malicious Files



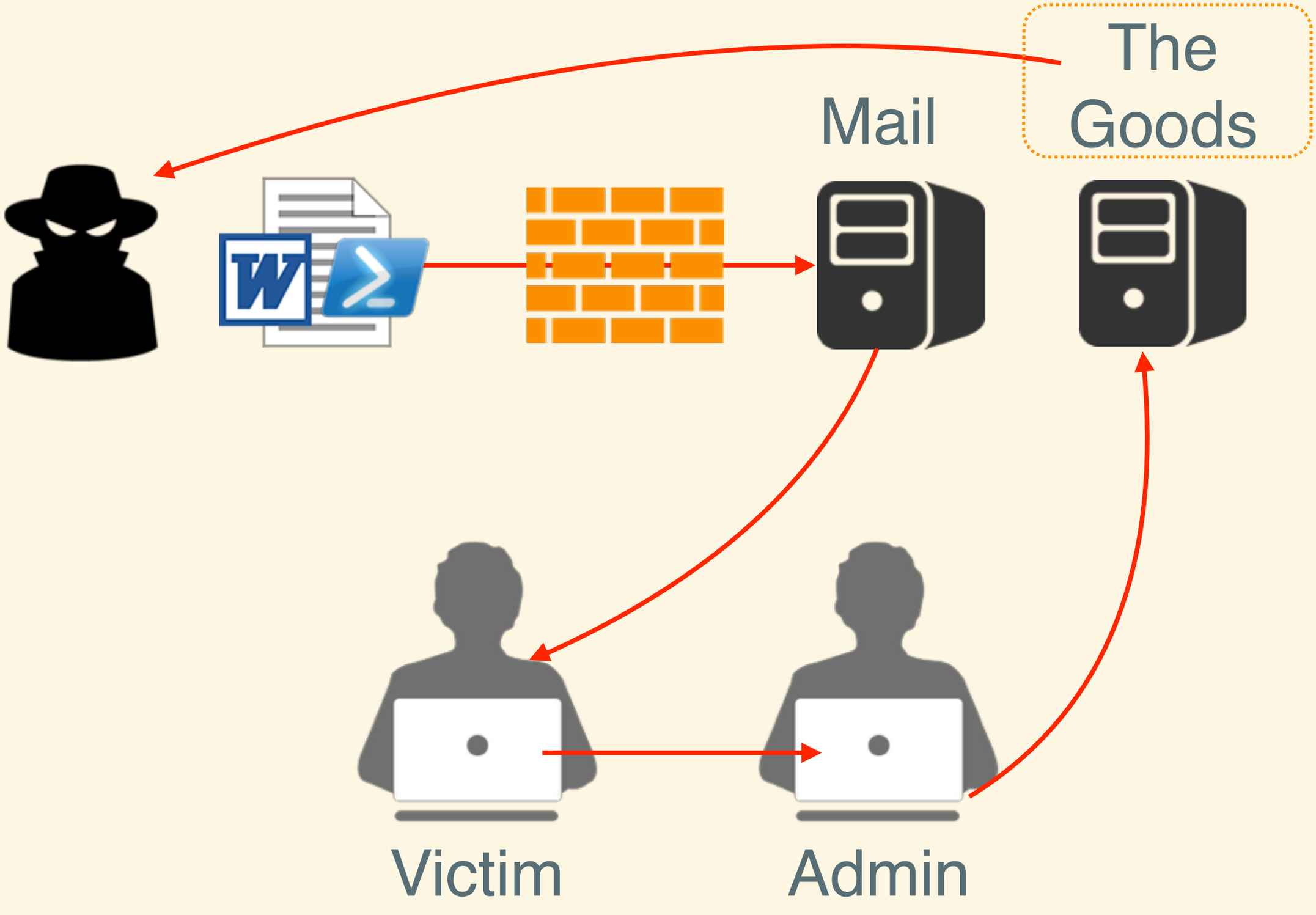
Lateral Movement



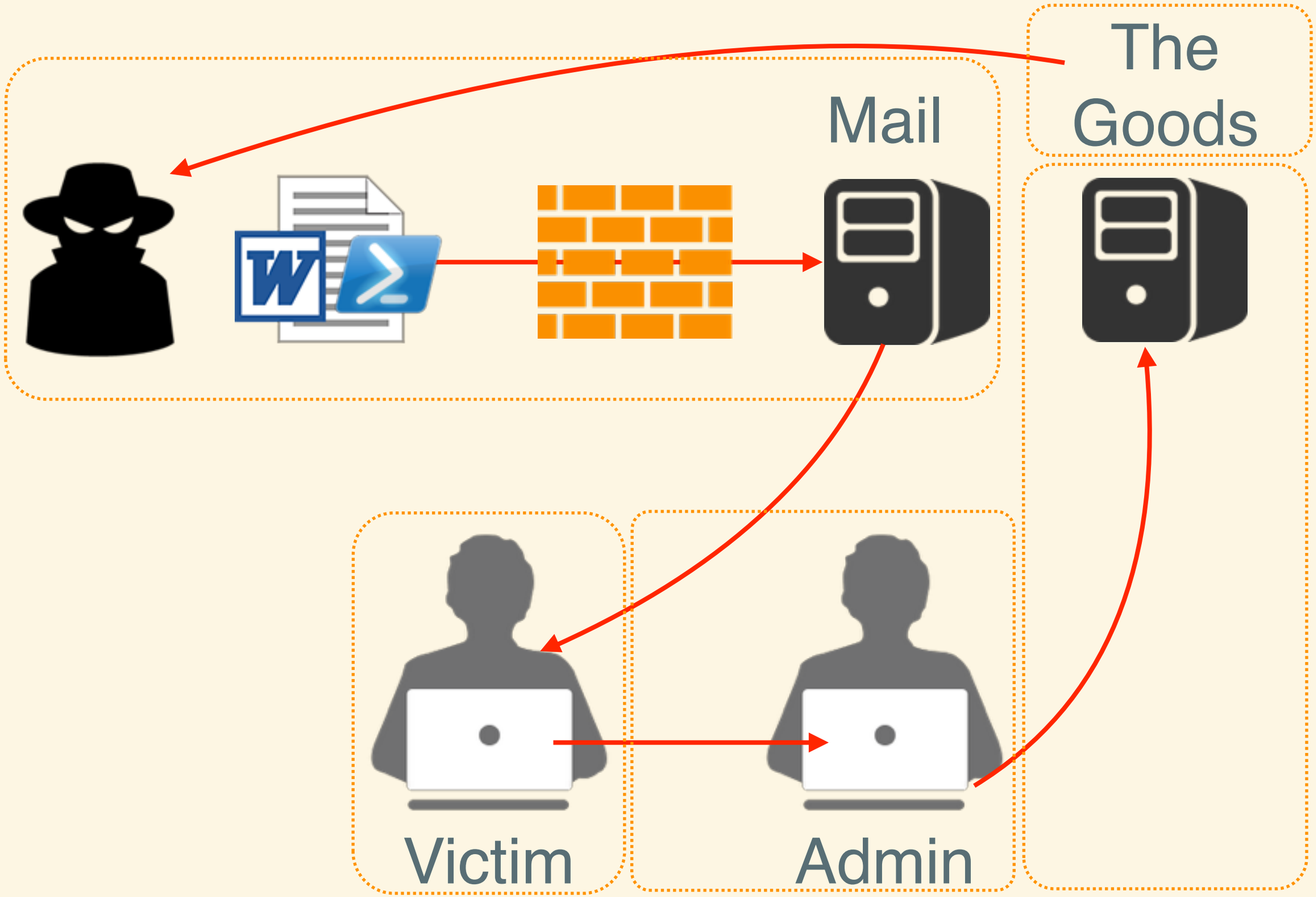
Unauthorized Server Access



Data Exfiltration



Do It Again



Simulation

- Each stage may be a sprint (2-4 weeks)
- Revalidate your controls
- Each technological gap is a business case opportunity

Tips For Offense

- Be a sparring partner
- Incorporate use cases into reports
- Provide more data like PCAPs
- Provide artifacts to reproduce attacks

Tips For Defense

- Build a backlog
- Require pen testing around your security stories
- Ask for more data from the tester
- Rotate your testing firms or rotate your testers

Thank You!

@ztgrace