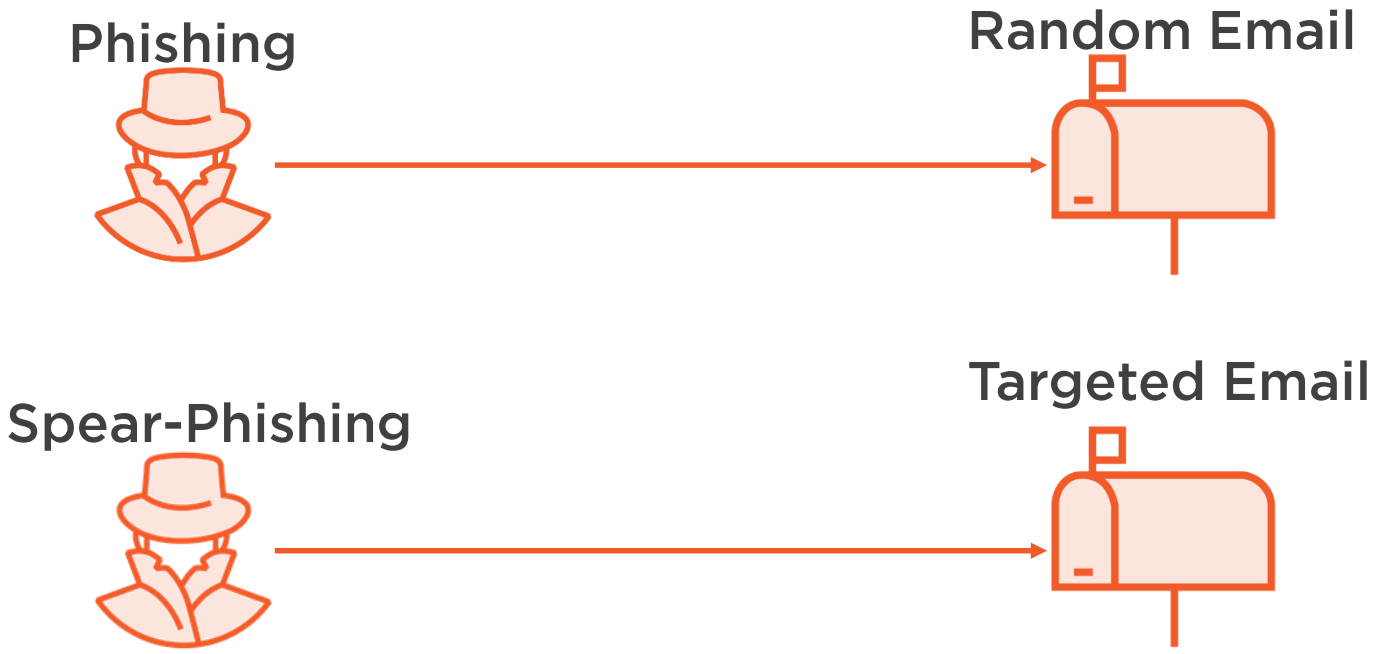
Spear-Phishing and Mailing Attacks

THE SOCIAL-ENGINEER TOOLKIT

Gus Khawaja

Gus.Khawaja@guskhawaja.me
www.ethicalhackingblog.com

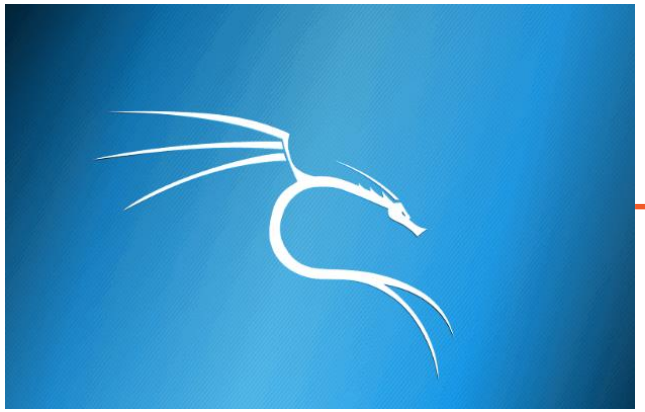
Phishing vs Spear-Phishing



Lab Setup

Attack Scenario

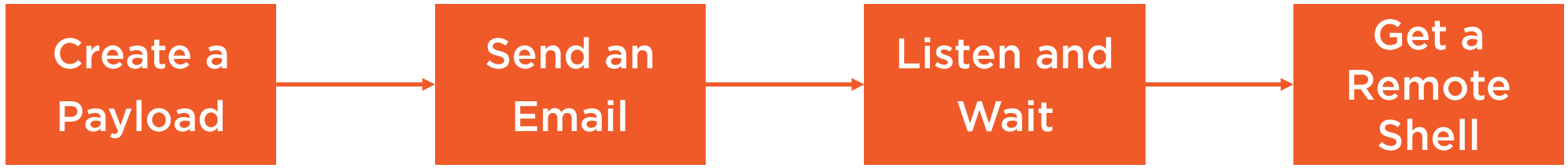
Attacker
OS: x64 Kali Linux 2017.1
IP: 192.168.0.102



Victim
OS: x86 Windows7
IP: 192.168.0.113

Create a Payload

Spear-Phishing Workflow



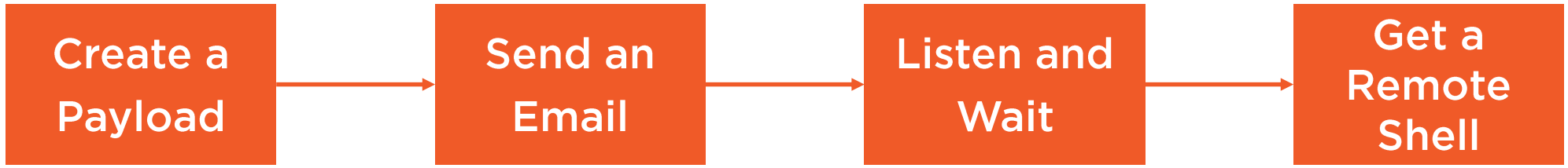
Payload

Don't use technology based payloads.

Use payloads that the OS will trust like **Powershell**.

Send an Email

Spear-Phishing Workflow



Email Spoofing

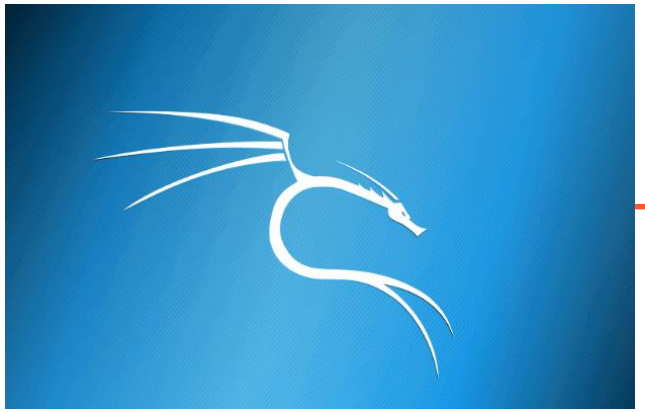
You need an SMTP relay account.

You need a convincing email message.

Email Attack Scenario

Attacker

Red Team Member: Gus Khawaja
Email Spoof: Microsoft Update Patch

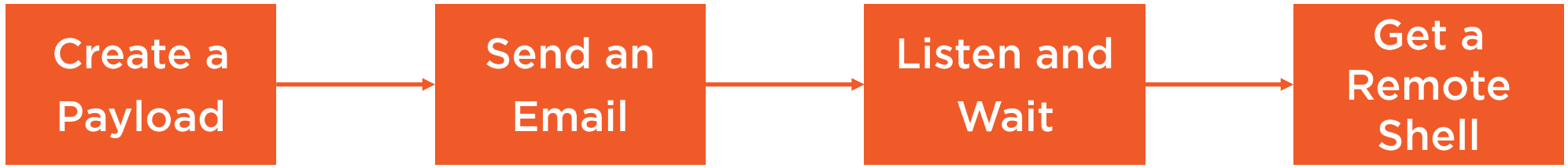


Victim

Employee: Admin
Company: Ethical Hacking Blog

Listen and Wait

Spear-Phishing Workflow



Remote Shell

Obfuscate the port number - 443

Use Metasploit & Meterpreter.

Summary

Spear-Phishing and Mailing Attacks

- Lab Tour
- Create the Payload
- Send the Email
- Listen and get a Remote Shell