Web Security & Bug Bounty: Networking Cheatsheet

For more courses, resources and workshop, visit zerotomastery.io

ZTM

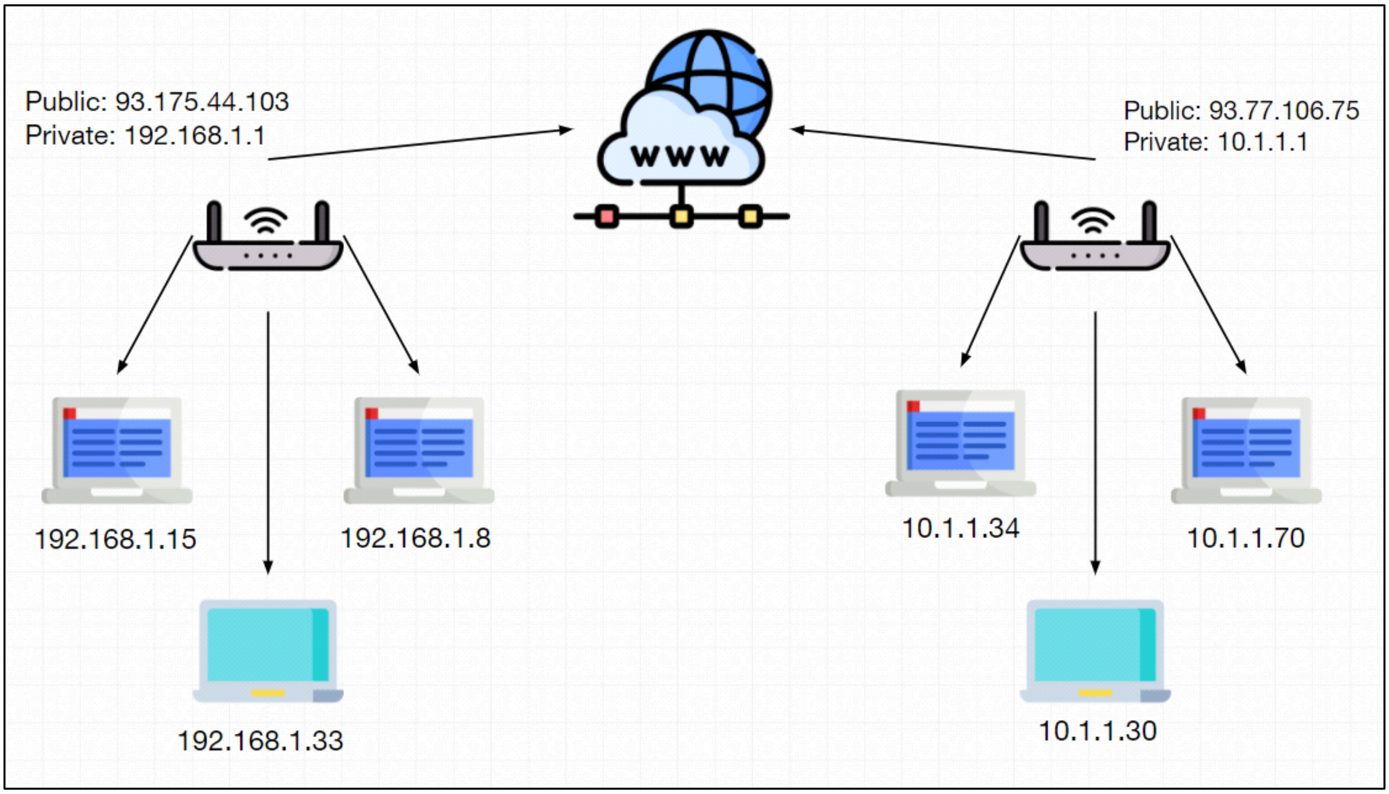
ACADEMY

Here you can find some of the networking terms/basics that we talk about throughout the course!

We will focus on important terms used for ***Bug Bounty/ Networking*** but we will also mention some other important terms that you must know as a ***Penetration Tester/Ethical Hacker***.

1) What is the difference between a public and private IP address?

All IPv4 IP addresses can be divided into two major groups: global, or public, or external - this group can also be called 'WAN addresses' — those that are used in the Internet, and private, or local, or internal addresses — those that are used in the local network (LAN).



1.1) Usually websites will be hosted on Public IP addresses unless they are in production. That is what allows us to type in a public IP inside of our search bar inside of a browser and it will load the website page. Inside the course we will be mostly attacking websites hosted on Local IPs from our Local Network. These type of webpages are only visible to devices inside of the network (unless they are connection forwarded through port forwarding or a tool used to forward the connection).

2) Public IP-address

It is public global addresses that are used in the Internet. A public IP address is an IP address that is used to access the Internet. Public (global) IP addresses are routed on the Internet, unlike private addresses.

The presence of a public IP address on your router or computer will allow you to organize your own server (VPN, FTP, WEB, etc.), remote access to your computer, video surveillance cameras, and access them from anywhere in the global network.

With a public IP address, you can set up any home server to publish it on the Internet: Web (HTTP), VPN (PPTP/IPSec/OpenVPN), media (audio/video), FTP, NAS network drive, game server, etc.

3) Private IP-address

Private internal addresses are not routed on the Internet and no traffic cannot be sent to them from the Internet, they only supposed to work within the local network.

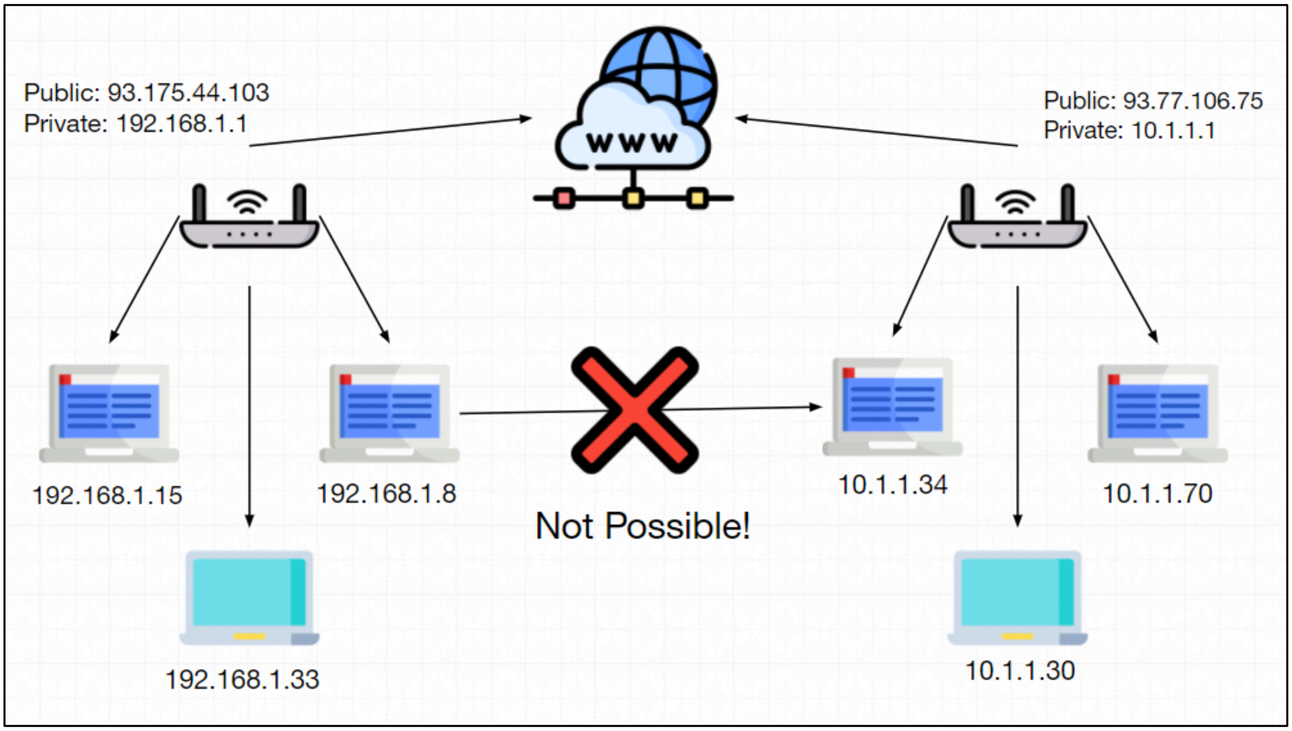
Private addresses include IP addresses from the following subnets:

Range from 10.0.0.0 to 10.255.255.255 — a 10.0.0.0 network with a 255.0.0.0 or an /8 (8-bit) mask

Range from 172.16.0.0 to 172.31.255.255 — a 172.16.0.0 network with a 255.240.0.0 (or a 12-bit) mask

A 192.168.0.0 to 192.168.255.255 range, which is a 192.168.0.0 network masked by 255.255.0.0 or /16

A special range 100.64.0.0 to 100.127.255.255 with a 255.192.0.0 or /10 network mask;



Direct Communication between these 2 is not possible!

4) What is DNS ?

Domain Name Server (DNS) is a standard protocol that helps Internet users discover websites using human readable addresses. Like a phonebook which lets you look up the name of a person and discover their number, DNS lets you type the address of a website and automatically discover the Internet Protocol (IP) address for that website.

Without DNS, the Internet would collapse - it would be impossible for people and machines to access Internet servers via the friendly URLs they have come to know.

5) What is DHCP ?

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring devices on IP networks, thus allowing them to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP. A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.

6) What is a Router ?

A router is a device that communicates between the internet and the devices in your home that connect to the internet. As its name implies, it “routes” traffic between the devices and the internet.

A router is a physical or virtual appliance that passes information between two or more packet-switched computer networks. A router inspects a given data packet's destination Internet Protocol address (IP address), calculates the best way for it to reach its destination and then forwards it accordingly.

A router is a common type of gateway. It is positioned where two or more networks meet at each point of presence on the internet. Hundreds of routers might forward a single packet as it moves from one network to the next on the way to its final destination.

7) Virtual Box Networking

Okay, had to add this in as it is important in setting up our environment and this is where 99% of issues occur!
All of the information about Virtual Box and its Network Settings you can actually find right here:
https://www.virtualbox.org/manual/ch06.html
But I am going to write the definition of 2 most important things for this course regarding Virtual Box Networking(these will be important once we actually set up our virtual machine and its network settings and also make sure to read about them on the link above in case you wonder how they work or what are their limitations):

7.1) NAT - Network Address Translation (NAT) is the simplest way of accessing an external network from a virtual machine. Usually, it does not require any configuration on the host network and guest system. For this reason, it is the default networking mode in Oracle VM VirtualBox.

A virtual machine with NAT enabled acts much like a real computer that connects to the Internet through a router. The router, in this case, is the Oracle VM VirtualBox networking engine, which maps traffic from and to the virtual machine transparently. In Oracle VM VirtualBox this router is placed between each virtual machine and the host. This separation maximizes security since by default virtual machines cannot talk to each other.

The disadvantage of NAT mode is that, much like a private network behind a router, the virtual machine is invisible and unreachable from the outside internet.

7.2) With bridged networking, Oracle VM VirtualBox uses a device driver on your host system that filters data from your physical network adapter. This driver is therefore called a net filter driver. This enables Oracle VM VirtualBox to intercept data from the physical network and inject data into it, effectively creating a new network interface in software. When a guest is using such a new software interface, it looks to the host system as though the guest were physically connected to the interface using a network cable. The host can send data to the guest through that interface and receive data from it. This means that you can set up routing or bridging between the guest and the rest of your network.

8) What are TCP & UDP ?

Actually this website explains it really well (we also do cover this inside of the course so you can wait for those lectures as well or you can learn it right now here!):
https://www.privateinternetaccess.com/blog/tcp-vs-udp-understanding-the-difference/

9) What is Bug Bounty ?

Bug bounty programs allow independent security researchers to report bugs to an organization and receive rewards or compensation. These bugs are usually security exploits and vulnerabilities, though they can also include process issues, hardware flaws, and so on.

10) What is HTTP ?

HTTP is a protocol which allows the fetching of resources, such as HTML documents. It is the foundation of any data exchange on the Web and it is a client-server protocol, which means requests are initiated by the recipient, usually the Web browser

11) What is a Client ?

The user-agent is any tool that acts on the behalf of the user. This role is primarily performed by the Web browser; other possibilities are programs used by engineers and Web developers to debug their applications.

To present a Web page, the browser sends an original request to fetch the HTML document that represents the page. It then parses this file, making additional requests corresponding to execution scripts, layout information (CSS) to display, and sub-resources contained within the page (usually images and videos). The Web browser then mixes these resources to present to the user a complete document, the Web page. Scripts executed by the browser can fetch more resources in later phases and the browser updates the Web page accordingly.

12) What is a Web Server ?

A web server stores and delivers the content for a website – such as text, images, video, and application data – to clients that request it. The most common type of client is a web browser program, which requests data from your website when a user clicks on a link or downloads a document on a page displayed in the browser.

A web server communicates with a web browser using the Hypertext Transfer Protocol (HTTP). The content of most web pages is encoded in Hypertext Markup Language (HTML). The content can be static (for example, text and images) or dynamic (for example, a computed price or the list of items a customer has marked for purchase). To deliver dynamic content, most web servers support server-side scripting languages to encode business logic into the communication. Commonly supported languages include Active Server Pages (ASP), Javascript, PHP, Python, and Ruby.