Scribe: Cryptography and Network Security (Class.9.B)

Vishal Gourav

20-Sep-2020

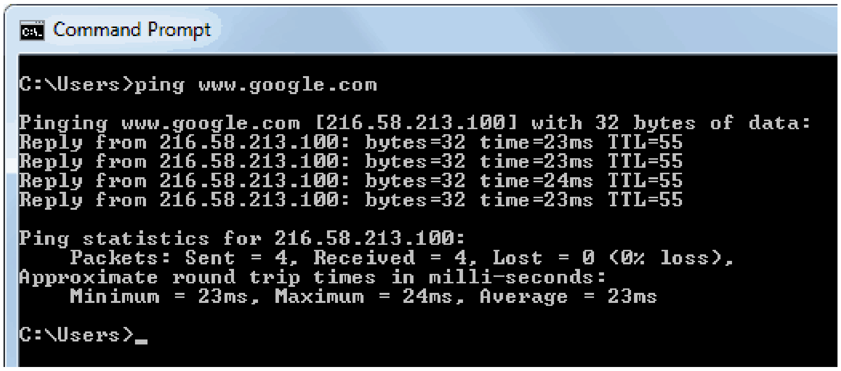
1 Introduction

We will be continuing the discussion on the basics of Computer Networks which is an integral pre-requisite for network threat modelling like, ping, traceroute, etc. Further we will be continuing the discussion on Number theory.

2 Network Scanning: PING

PING is a low level network utility command used to check connectivity of a given address which might be a web address or an IP address. Some properties can be listed as follows:-

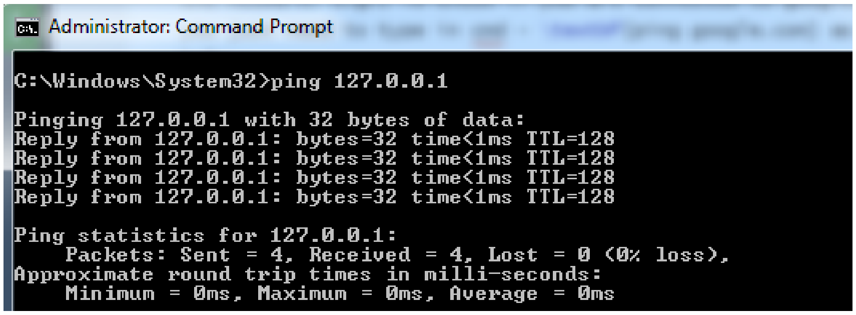
- PING stands for- Packet Internet Groper
- It can be used to check connectivity of a given device to the network. e.g., To check if you are connected to google.co.in you just need to type in cmd - **ping google.com** as shown below:-



```
C:\Users>ping www.google.com

Pinging www.google.com [216.58.213.100] with 32 bytes of data:
Reply from 216.58.213.100: bytes=32 time=23ms TTL=55
Reply from 216.58.213.100: bytes=32 time=23ms TTL=55
Reply from 216.58.213.100: bytes=32 time=24ms TTL=55
Reply from 216.58.213.100: bytes=32 time=23ms TTL=55

Ping statistics for 216.58.213.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 24ms, Average = 23ms

C:\Users>_
```

Figure 1: Ping google using cmd

- PING can also be used to check self connectivity using special address 127.0.0.1 as given in Figure 2.



```
C:\Windows\System32>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

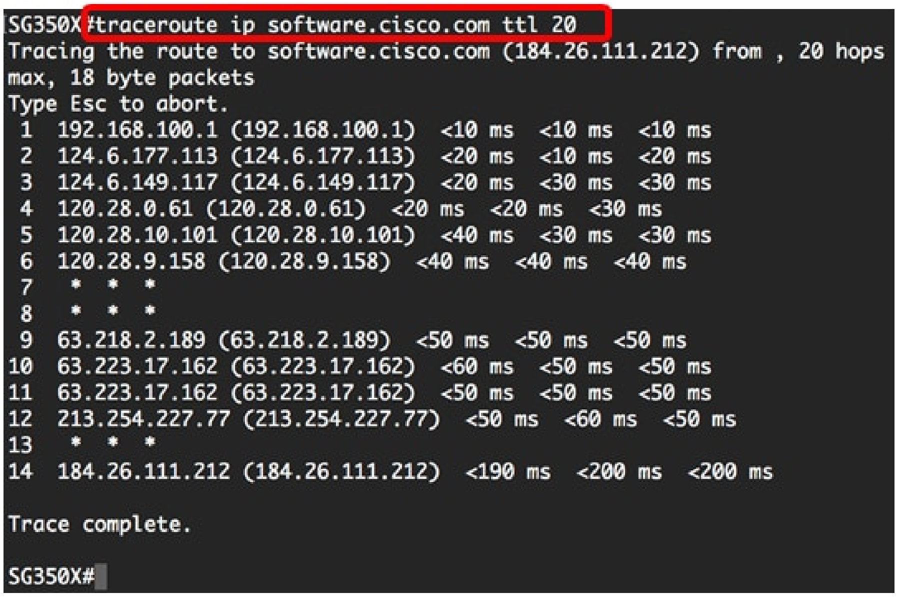
Figure 2: Ping for checking self connectivity using cmd

- It is an ICMP message and by default is 56 Bytes long and can be a maximum of 65536 Bytes.
- An interesting thing to note here is that a ping packet of size greater than 65536 bytes may cause a buffer overflow.This phenomenon is reffered to as th **PING of Death**.

3 Network Routing: Traceroute

Next we come to traceroute. It is a feature used by a sender to know the route that a packet sent by him/her is taking on path to the destination. It can be further explained as follows:-

- It uses TTL field in the IPv4 header to carry out the routing process.
- It starts sending out packets iteratively with increase in TTL value from $1, 2, 3 \ldots\ldots n$. What happens is that, the routers in between on seeing a packet with TTL$=0$ send back a **Time Limit Exceeded** ICMP packet which contains the router's IP address as sender data and thus, when traceroute receives this ICMP it finds out the router's address.
- It should be noted that the traceroute may contain empty addresses because the ICMP packets sent by the routers may be dropped to reduce congestion in the path as in Figure-3.
- Furthermore, The route received may not always be the exact route taken by an actual packet because different packets may take different paths



```
SG350X#traceroute ip software.cisco.com ttl 20
Tracing the route to software.cisco.com (184.26.111.212) from , 20 hops
max, 18 byte packets
Type Esc to abort.
 1  192.168.100.1 (192.168.100.1)  <10 ms  <10 ms  <10 ms
 2  124.6.177.113 (124.6.177.113)  <20 ms  <10 ms  <20 ms
 3  124.6.149.117 (124.6.149.117)  <20 ms  <30 ms  <30 ms
 4  120.28.0.61 (120.28.0.61)  <20 ms  <20 ms  <30 ms
 5  120.28.10.101 (120.28.10.101)  <40 ms  <30 ms  <30 ms
 6  120.28.9.158 (120.28.9.158)  <40 ms  <40 ms  <40 ms
 7   *  *  *
 8   *  *  *
 9  63.218.2.189 (63.218.2.189)  <50 ms  <50 ms  <50 ms
10  63.223.17.162 (63.223.17.162)  <60 ms  <50 ms  <50 ms
11  63.223.17.162 (63.223.17.162)  <50 ms  <50 ms  <50 ms
12  213.254.227.77 (213.254.227.77)  <50 ms  <60 ms  <50 ms
13   *  *  *
14  184.26.111.212 (184.26.111.212)  <190 ms  <200 ms  <200 ms

Trace complete.

SG350X#
```

Figure 3: A typical Traceroute

4 Port Scanning: nmap

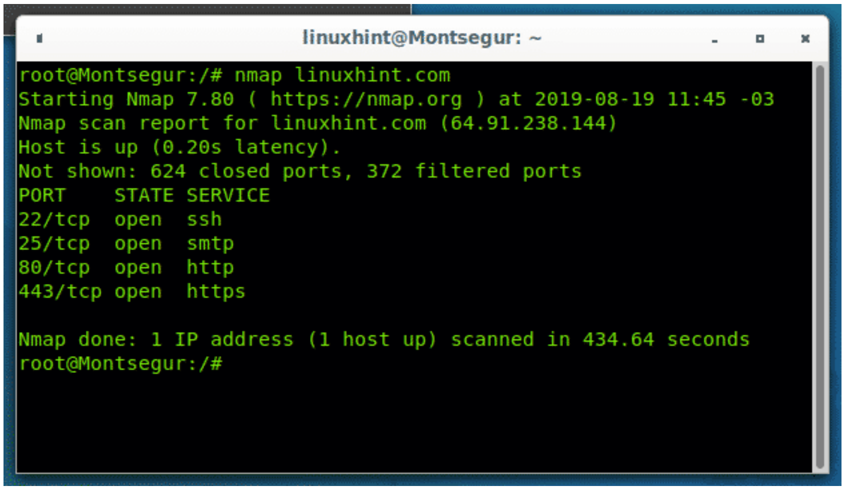
A **port scan** is a method for determining which ports on a network are open. As ports on a computer are the place where information is sent and received, port scanning is analogous to knocking on doors to see if someone is home.Some further illustrations are as follows:-

- **A port scanner** is an application designed to probe a server or host for open ports. Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.
- These scans reveal the presence of security in place such as a firewall between the server and the user's device.
- The general protocols used for port scanning are TCP (transmission control protocol) and UDP (user datagram protocol).
- A port scan may indicate as indicated in Figure-4:-

  Open ports

  Closed ports

  Filtered ports



```
root@Montsegur:/# nmap linuxhint.com
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-19 11:45 -03
Nmap scan report for linuxhint.com (64.91.238.144)
Host is up (0.20s latency).
Not shown: 624 closed ports, 372 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 434.64 seconds
root@Montsegur:/#
```

Figure 4: Nmap working

5 Number Theory

We already have discussed what algebraic structure, semigroup and monoid are. So we will be covering Group,Ring and Field.

5.1 Group

- A monoid can be further classified as a **Group** if for given $(S, \diamond)$, $\forall x \in S$ there exists $\exists y$ such that, $x \diamond y = e$ (where e is the identity element of R)
- In simple words for every element an **inverse** must exist.
- Example: $(Z, +)$, $(R, *)$
- The group is further labelled an **Abelian Group** if it is commutative i.e., $\forall x, y \in S$:-
$$x \diamond y = y \diamond x \tag{1}$$

5.2 Ring

- A ring is a triplet $(R, +, .)$ such that $(R, +)$ is an **Abelian Group** and $(R, .)$ is a **Monoid**.
- The ring is called commutative if the semigroup $(R, .)$ is commutative.
- It is further called a **Residual Class Ring** or **Quotient ring** if it is distributive over first operator i.e., $\forall x, y, z \in R$:-
$$x.(y + z) = (x.y) + (x.z) \tag{2}$$

5.3 Zero Divisor

- An element $x \in R$ is called a **Zero Divisor** if it is nonzero and there is x nonzero y in R, st. $xy = 0$ or $yx = 0$ i.e., $\forall x, y \in R such that x \neq 0 and y \neq 0$:-

$$x.y = 0 \ or \ y.x = 0 \tag{3}$$

- The zero divisors of the residue class $\mathbf{Z}/m\mathbf{Z}$ is $a{+}m\mathbf{Z}$, with $1 < gcd(a, m) < m$.

- **Proof.** Suppose that $n > 2$ and that n is a composite number. Then n has a non-negative divisor d such that $1 < d < n$. There are two cases to consider.
  Case 1:
  Suppose that d is the only divisor of n such that $d \neq 1$ and $d \neq n$. Then we must have that $d^2 = n$. Therefore for $[d]_n \neq [0]_n$ we have that:

$$[d]_n * [d]_n = [d]_n = [d^2]_n = [n]_n = [0]_n \tag{4}$$

  Therefore [d]n is a zero divisor of Z/nZ.

  Case 2: Suppose that d is not the only divisor of n such that $d \neq 1$ and $d \neq n$. Then there must exist another divisor k such that $k \neq 1$ and $k \neq n$ where $d * k = n$. Therefore for $[d]_n$,$[k]_n \neq [0]_n$ we have that:

$$[d]_n * [k]_n = [d * k]_n = [n]_n = [0]_n \tag{5}$$

  Therefore $[d]_n$ and $[k]_n$ are zero divisors of $\mathbf{Z}/n\mathbf{Z}$.Thus, if $n > 2$ is composite then $\mathbf{Z}/n\mathbf{Z}$ has a zero divisor.

- **Corollary.** If p is prime,then $\mathbf{Z}/p\mathbf{Z}$ has no zero divisors.

5.4 Field

- A field is a commutative ring $(R, +, .)$ in which every element in the semigroup $(R, .)$ is invertible i.e., $\forall x \in R$ there must exist $\exists y \in R$ such that:-

$$x.y = e \tag{6}$$

- Example: Set of Real numbers($\mathbf{R}$).

6 Conclusion

We have discussed here about some basics of computer networks and Number Theory.