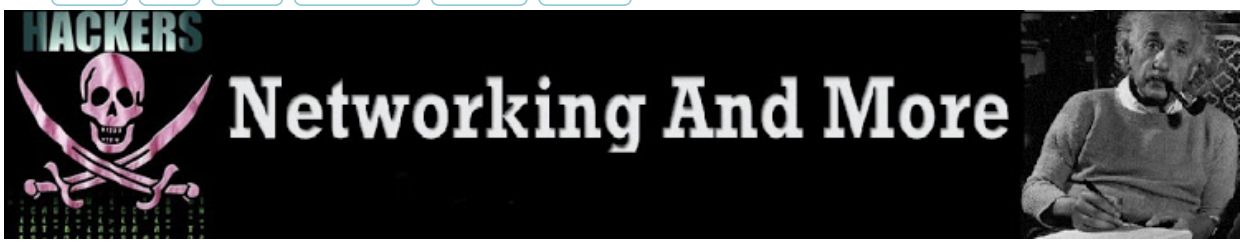
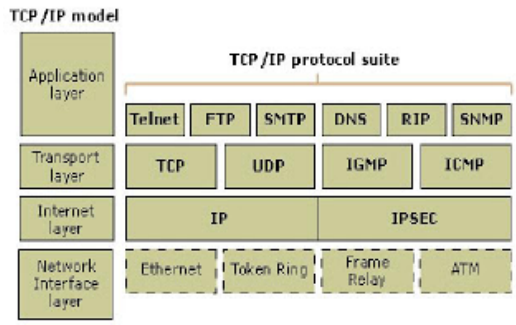



I have learned PHP the hard way. I just bumped into PHP by chance and fell in love with it since I realized its true power. I learn a lot of stuff everyday and I will try and document most of them here.

4/07/2011

## Understanding TCP/IP using Wireshark


I feel that it is best to use a packet sniffing tool like wireshark to understand TCP/IP. The following picture shows the layers of TCP/IP and the protocols involved.




Almost everybody would have learned this in college, but lets take this a step further.

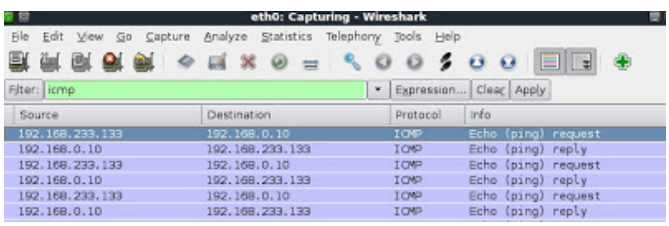
First, I ping my Win 7 machine from my VM, Backtrack

IP of Windows 7 is **192.168.0.10**

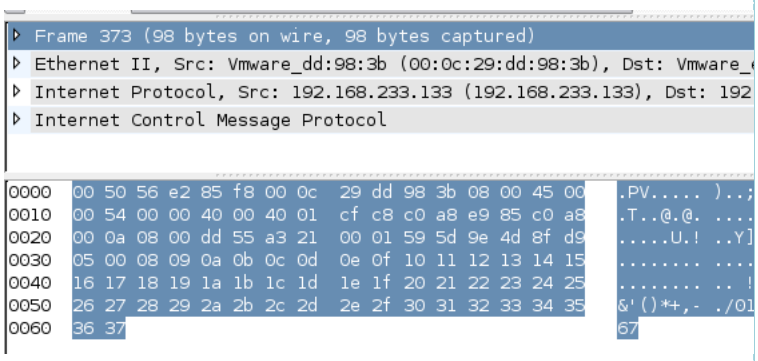
IP of Backtrack is **192.168.233.133**

```
root@bt:~# ping 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=128 time=3.67 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=128 time=2.07 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=128 time=1.87 ms
```

I have set my wireshark to capture only ICMP packets, as you would know ping is an ICMP packet



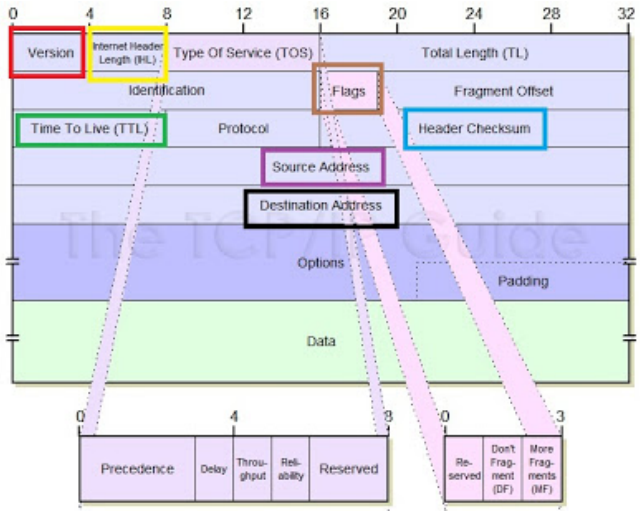

you can see the request from my backtrack, 233.133 to win7, 0.10 (echo ping request and reply)
Now lets take a closer look at the echo request




You can see the source and destination, the ICMP and HEX values of the packet. Every protocol has a HEX value, as the picture shows below

| Value (Hexadecimal) | Value (Decimal) | Protocol |
|---|---|---|
| 00 | 0 | Reserved |
| 01 | 1 | ICMP |
| 02 | 2 | IGMP |
| 03 | 3 | GGP |
| 04 | 4 | IP-in-IP Encapsulation |
| 06 | 6 | TCP |
| 08 | 8 | EGP |
| 11 | 17 | UDP |
| 32 | 50 | Encapsulating Security Payload (ESP) Extension Header |
| 33 | 51 | Authentication Header (AH) Extension Header |

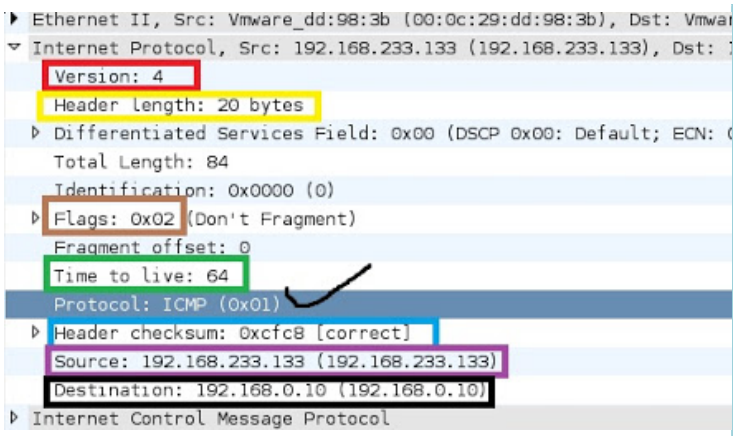
As you can see, ICMP is 01 (keep this in mind)
Now comes the most important part, this is a typical TCP/IP packet




Now lets investigate the packet using wireshark by expanding the Internet Protocol portion, i.e, the third row of the ICMP packet captured by wireshark

Note: **I have used the same colour to represent the corresponding portion a general TCP/IP packet and the ICMP packet that I sent.**

Puzzle 8:Shiekh's inheritence
Puzzle 7: Christmas Tree
Puzzle 6: Head Bands
Puzzle 5: The Magnet
Backtrack, a must have for hacking enthusiasts
If you are having problems with loading your gmail...
Useful ports and port numbers
SSH Using Public Key Cryptography
Public key authentication
Puzzle 4: Masters of Logic 3
Puzzle 3: Masters of Logic 2
Puzzle 2: Masters of Logic 1
My favourite puzzles 1: Guess my B'day
SSH
Backup using dd
First Post - Gmail Motion




You can see the details of the packet. The version is IPv4, the protocol is ICMP with its HEX(01), as depicted by my earlier diagram, and so on.

I believe wireshark is a great tool for learning this kind of stuff and is a must have. I will come up with a tutorial on wireshark in the near future.

Posted by Indrajith at 18:46

### 1 comment:

**Vivek Menon** 28 June 2013 at 05:25

nice post. clear and concise explanation. the coloring helps a lot

Reply

Enter your comment...

Comment as: GeeKer (Google) Sign out

Publish Preview Notify me

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)