Detect/Analyze Scanning Traffic Using Wireshark

"Wireshark", the world's most popular Network Protocol Analyzer is a multipurpose tool. It can be used as a Packet Sniffer, Network Analyser, Protocol Analyser & Forensic tool. Through this article my focus is on how to use Wireshark to detect/analyze any scanning & suspect traffic.

Let's start with Scanning first. As a thief studies surroundings before stealing something from a target, similarly attackers or hackers also perform foot printing and scanning before the actual attack. In this phase, they want to collect all possible information about the target so that they can plan their attack accordingly. If we talk about scanning here they want to collect details like:

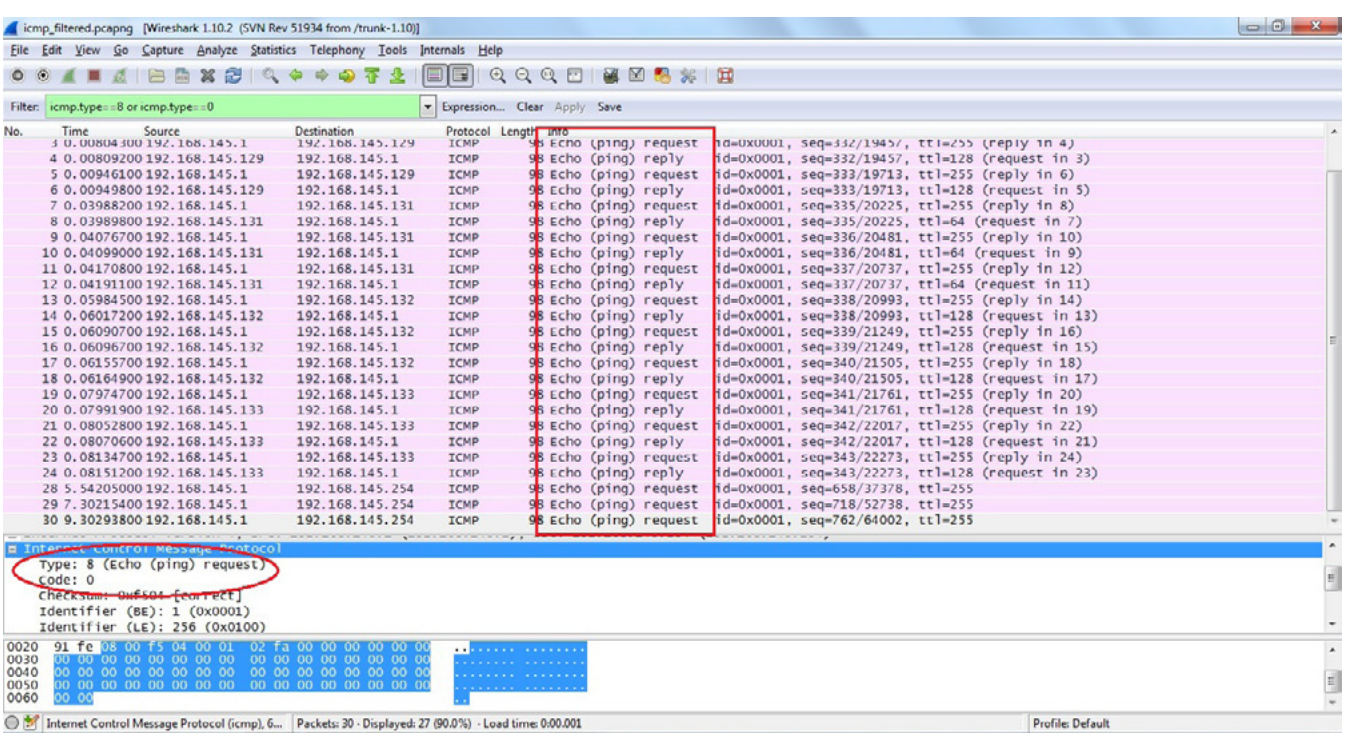

Figure 1. *Ping Sweep*

- Which IP addresses are in use?
- Which port/services are active on those IPs?
- Which platform (Operating System) is in use?
- What are the vulnerabilities & other similar kinds of information.
- Now I am moving to some popular scan methods and how to detect them in Wireshark.

Ping Sweep

This scan is helpful to find out which IPs are active in the network. Ping Sweep can be performed using ICMP, TCP or UDP, the most popular one is ICMP Ping Sweep. In this ICMP type 8, ECHO request is followed by ICMP type 0, ECHO reply packets are being used while in TCP/UDP ping sweep packets are destined to TCP/UDP port 7, The ECHO port. If that target host doesn't support ECHO service then this TCP/UDP ping sweep will not work. Thus ICMP ping sweep is mostly used, but if there is a firewall in between which is configured to block ICMP packet then even ICMP ping sweep is useless. In this situation, ARP scan/ARP sweep can be used which is discussed next (Figure 1).

To detect ICMP ping sweep in Wireshark apply simple filter `icmp.type==8 or icmp.type==0`. TCP ping sweep can be detected with `tcp.dstport==7` filter and for UDP ping sweep `udp.dstport==7` filter can be used. After applying these filters if we are getting more than expected packets then it's possible that ping sweep is going on in our network. We need to be careful about the volume of such traffic as it might be normal ping traffic. It should be considered as a scan signature only if you are getting unexpected increase in ICMP traffic.

ARP Sweep/ARP Scan

As discussed in previous scan that if a firewall is implemented in between and ICMP is blocked then we can't use ICMP ping sweep. In such a situation, ARP scan is helpful to find out active IPs in the network. Here, attacker sends ARP broadcast (for broadcast, destination MAC will be `0xff:ff:ff:ff:ff:ff`) for each and every possible IP in selected subnet and if he gets ARP response then it shows that IP is active. Advantage of this scan is that ARP communication can't be filtered or disabled because all TCP/IP communication is based on it. Blocking or disabling ARP communication will break TCP/IP communication or it will force static ARP entries and disadvantage of this scan is that it can't cross layer 3 Devices. This scan can be easily detected with filter ARP. After applying this filter if we are getting unexpected no. of ARP queries as shown in the picture, it is a sign for ARP scan or ARP sweep (FIgure 2).

TCP Half Open/Stealth Scan

To detect open or close TCP port on target system, Stealth scan is the most often used method. In this scan, attacker sends a SYN packet on the target

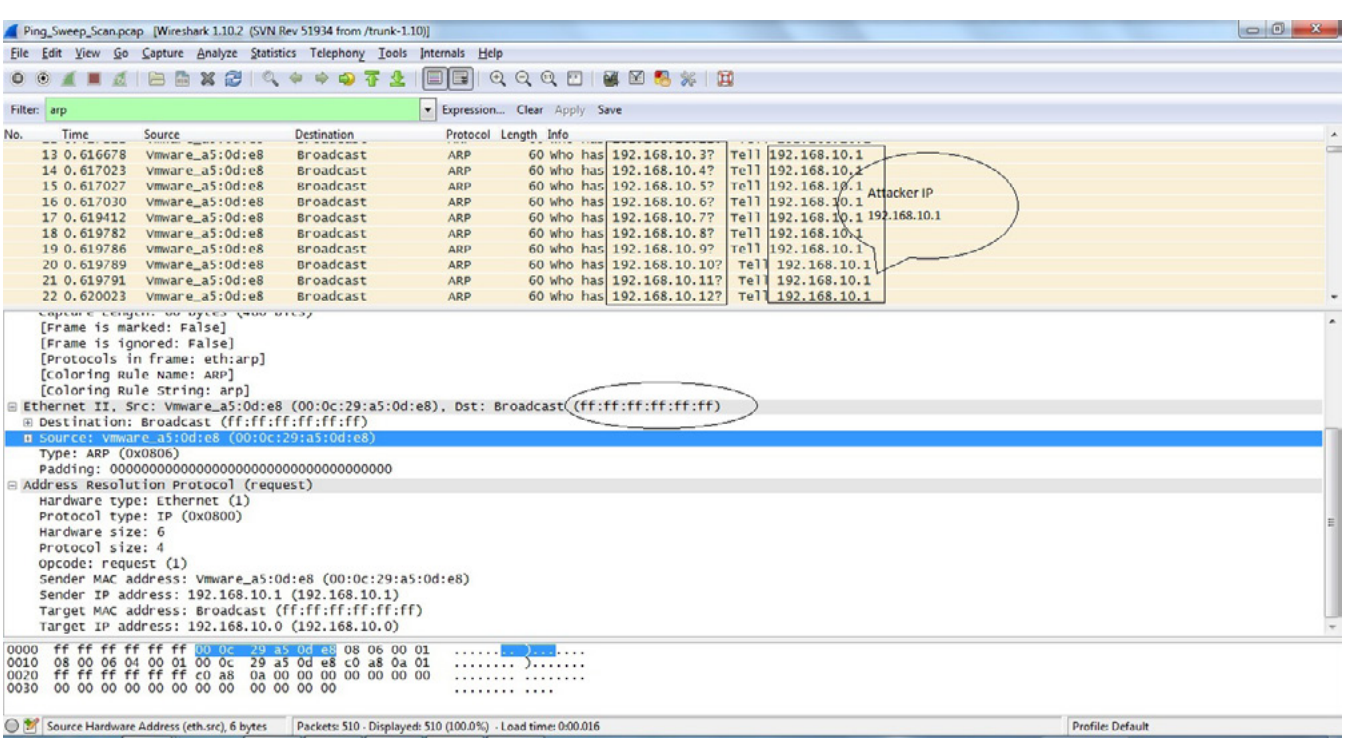

Figure 2. *ARP Scan/ARP sweep*

port like a normal TCP communication. If the port is open, he will get SYN+ACK and RST or RST+ACK if the port is closed. After getting SYN+ACK on the open port as a response, attacker will send RST because attacker doesn't want to open TCP session with a target. If that target port is firewalled then expected response is ICMP type 3 Packet with Code 1,2,3,9,10, or 13. So in Wireshark if we are getting a lot of RST packets or ICMP type 3 packets, it can be a sign for Stealth Scan or TCP Full Connect Scan. As we can see that in the above picture a lot of SYN & RST packets are moving back and forth, but there is no data communication between these hosts. To get a quick view in the above capture we can go to top menu Statistics -> Conversations and then go to TCP tab. There we can see multiple TCP sessions, but all are having less than 4 packet communications which is a sign for TCP port Scan (Figure 4).

TCP Full Connect Scan

In this scan attacker is going to perform complete three way hand shake to find out if the port is open

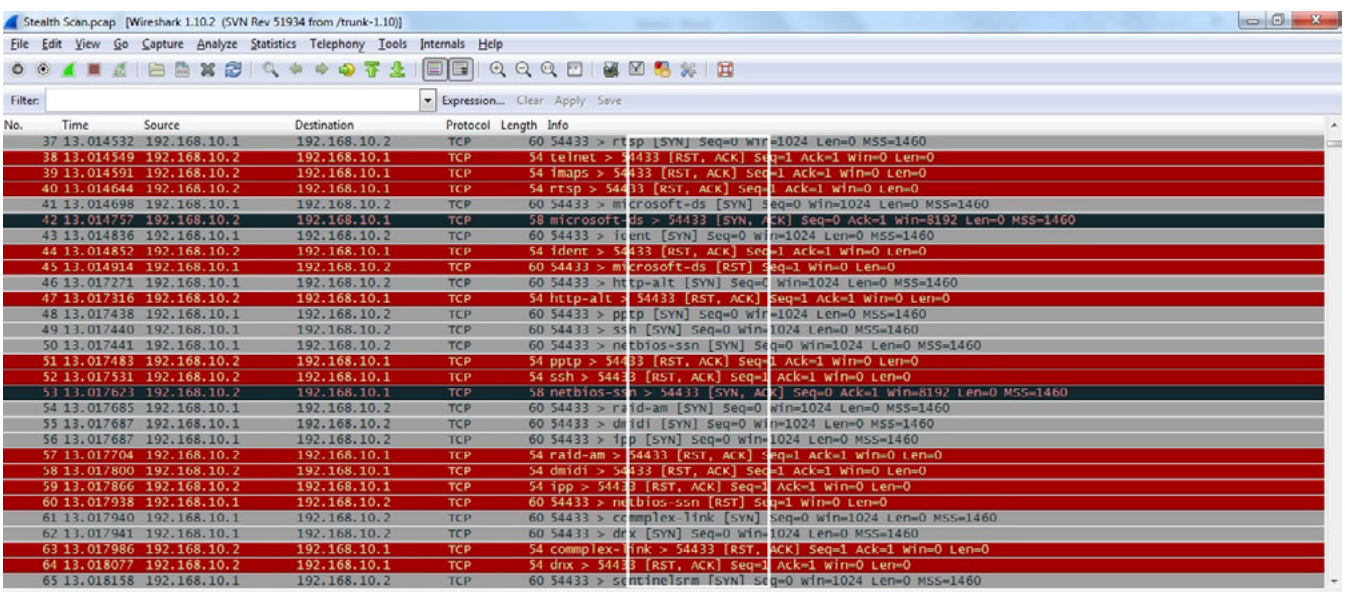

Figure 3. *Stealth Scan*

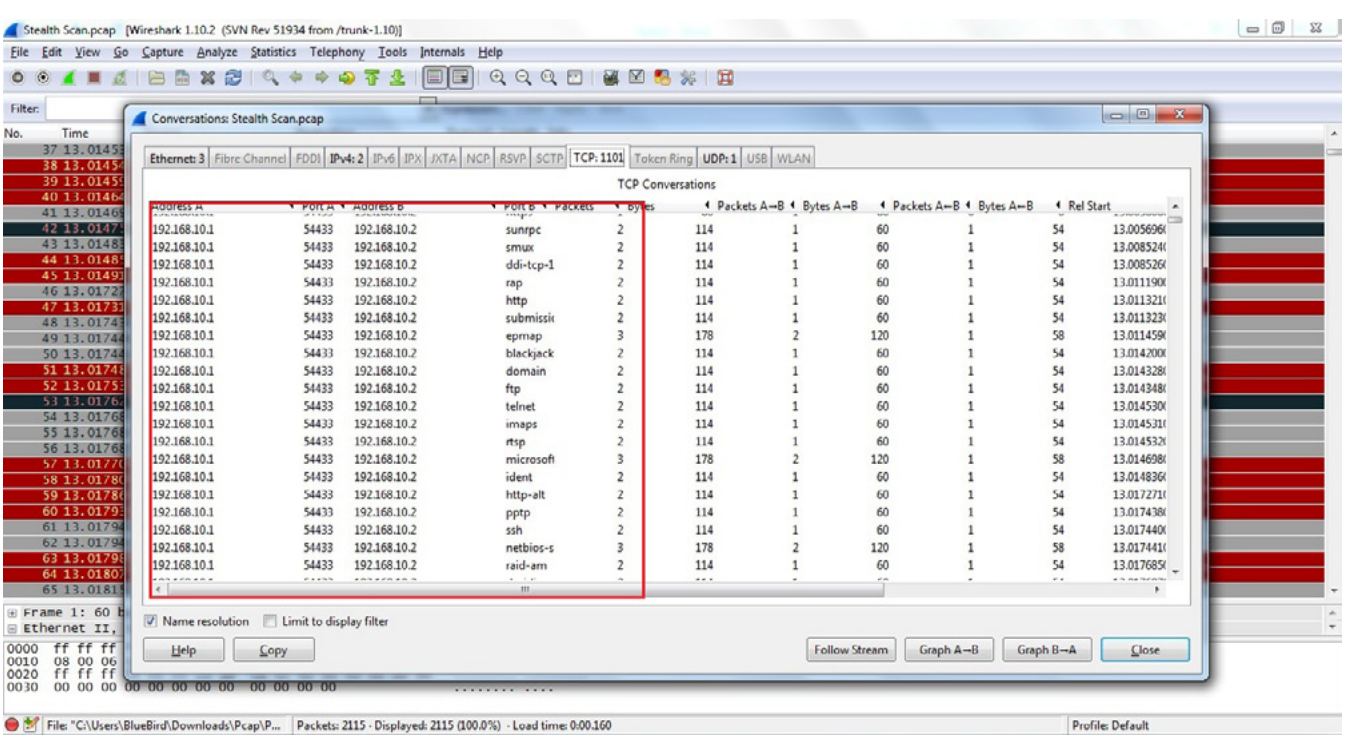

Figure 4. *Statistics->Conversation_ TCP tab*

or close. Attacker will send SYN on target port, if the port opens, he will get SYN+ACK and RST+ACK on the closed port. After getting SYN+ACK, the attacker will send ACK and try to establish TCP session and then terminate it. In Wireshark, we can use a similar method like TCP Half open scan to detect TCP full connect as well. If that target port is firewalled then here also we will get the same response which is ICMP type 3 Packet with Code 1,2,3,9,10, or 13. Following filters can be used in Wireshark to detect TCP scan packet quickly (TCP Half open & TCP Full Connect)

- To get SYN, SYN+ACK, RST & RST+ACK packet

```
tcp.flags==0x002 or tcp.flags==0x012 or tcp.
   flags==0x004 or tcp.flags==0x014
```

- To get ICMP type 3 Packet with Code 1,2,3,9,10, or 13 Packet

```
icmp.type==3 and (icmp.code==1 or icmp.code==2 or
   icmp.code==3 or icmp.code==9 or icmp.code==10
   or icmp.code==13)
```

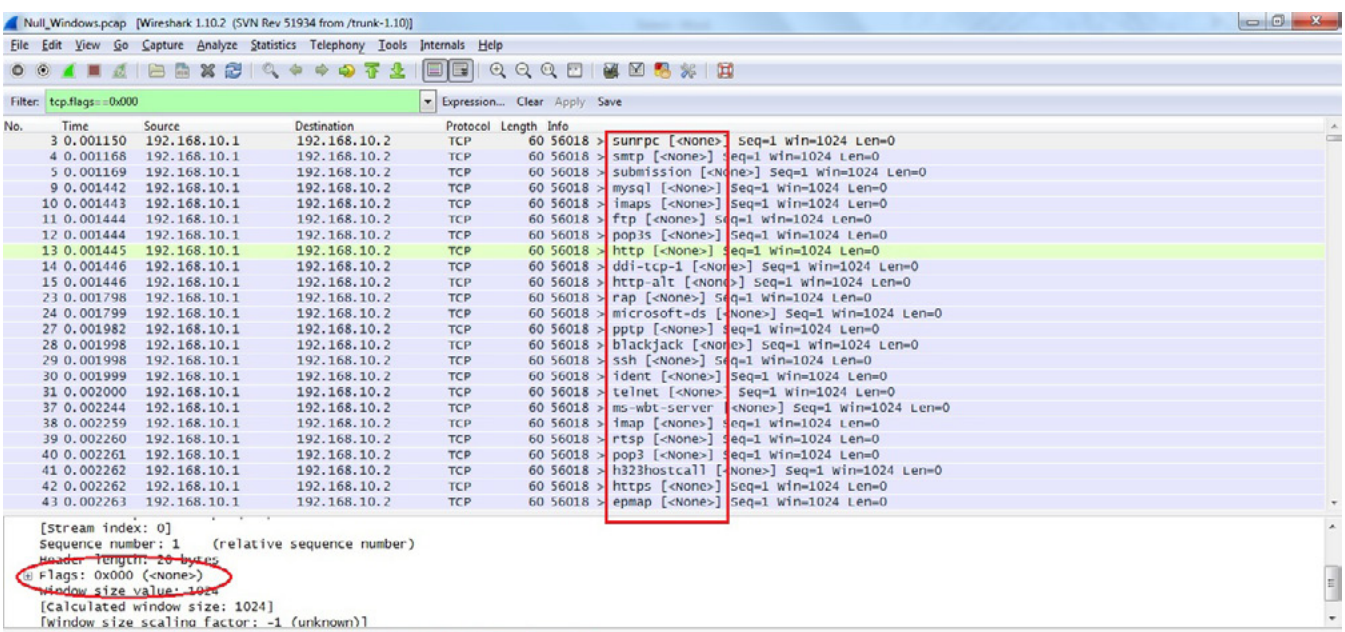

Figure 5. *TCP Null Scan*

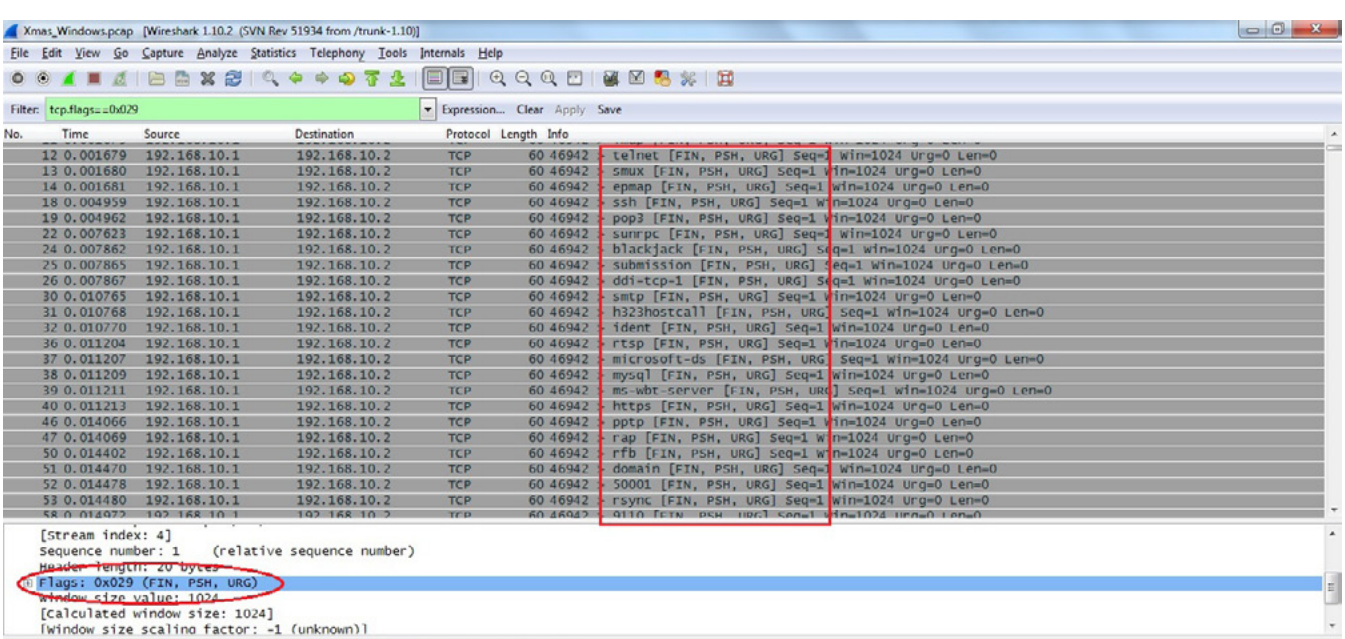

Figure 6. *TCP Xmas Scan*

- To get SYN, SYN+ACK, RST & RST+ACK packet along with ICMP type 3 Packet with Code 1,2,3,9,10, or 13 Packet

```
tcp.flags==0x002 or tcp.flags==0x012 or tcp.
   flags==0x004 or tcp.flags==0x014 or (icmp.type==3
   and (icmp.code==1 or icmp.code==2 or icmp.
   code==3 or icmp.code==9 or icmp.code==10 or
   icmp.code==13))
```

Null Scan

In this scan attacker sends a TCP packet without setting any flag on it and as a response if he is getting RST packet it means the port is closed.

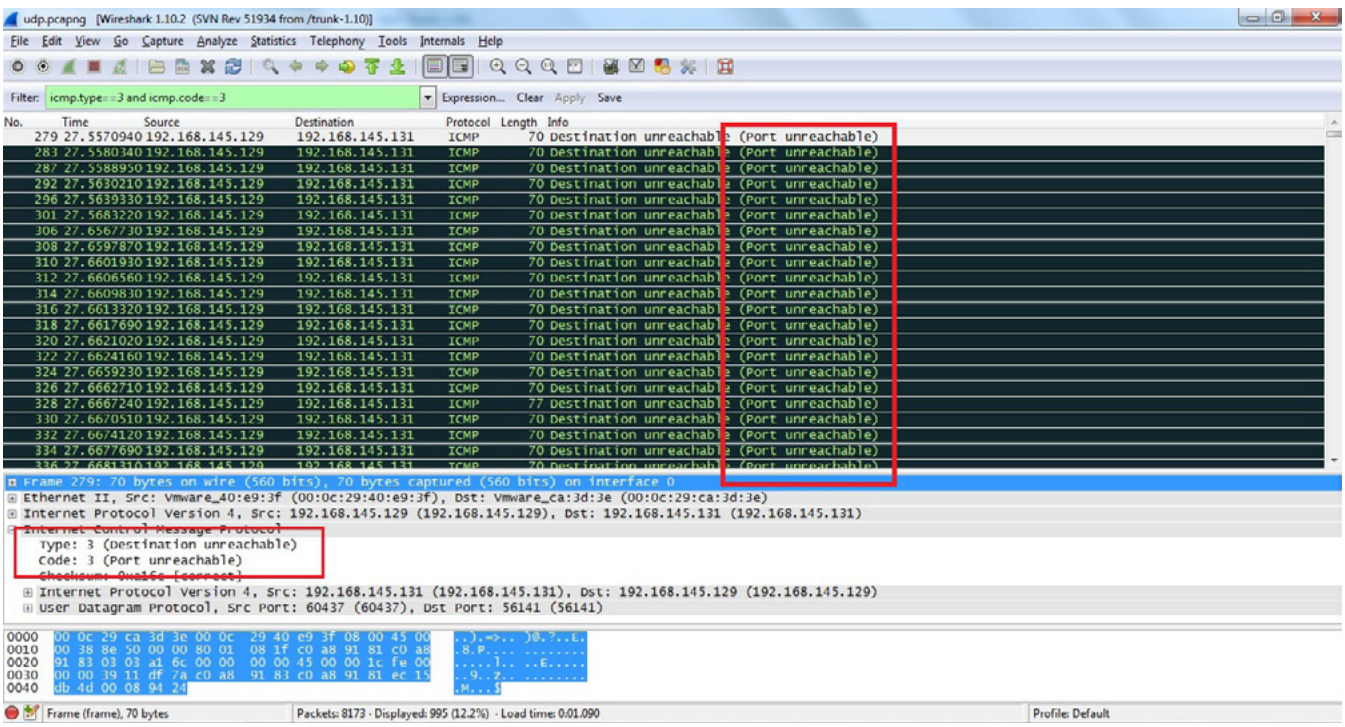

Figure 7. *UDP Scan*

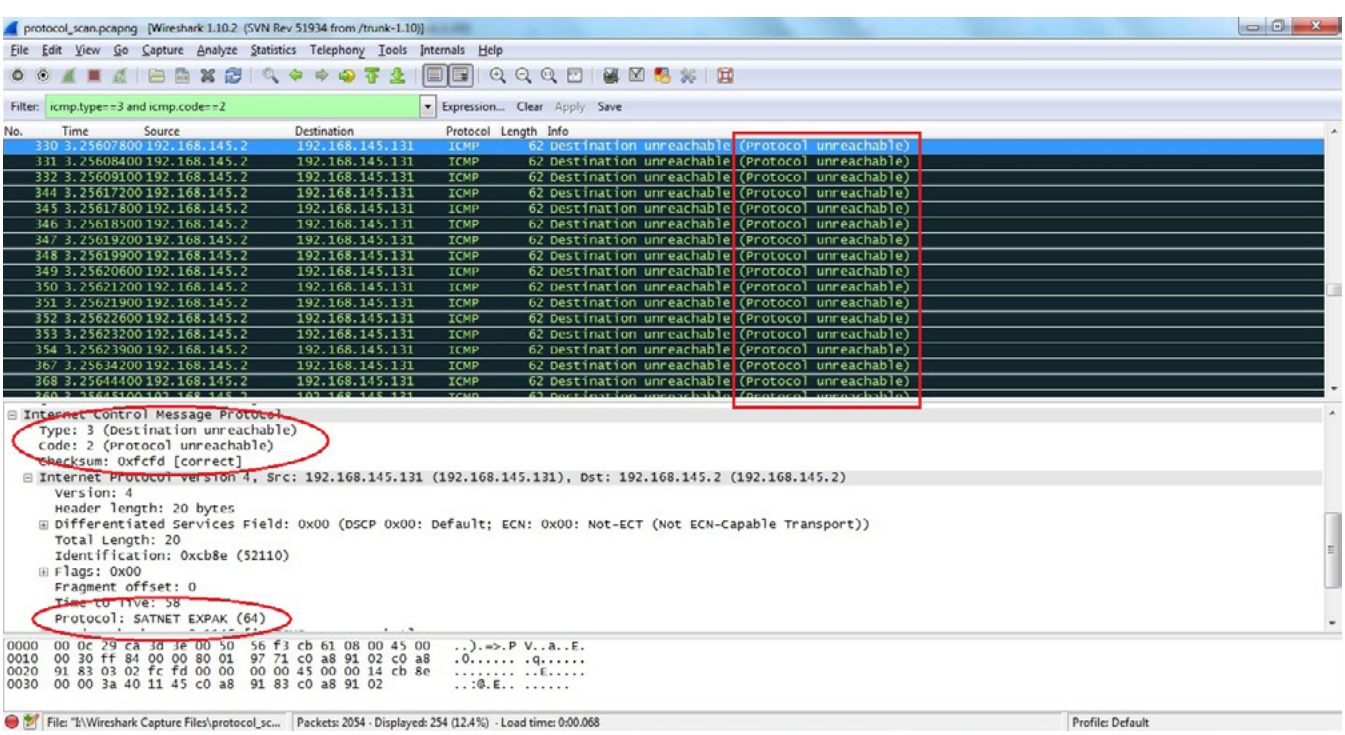

Figure 8. *Protocol Scan*

There will be no response to null scan if the port is open or filtered and if he is getting ICMP Type 3 Code 1,2,3,9,10 or 13 packet then *port seems to be firewalled.To detect Null Scan in Wireshark, we can use a simple filter* `TCP.flags==0x000`. It will filter all TCP packets moving without Flag (Figure 5).

Xmas Scan

Here the attacker sends packet with FIN, PSH & URG TCP flags and response is exactly the same like Null Scan. To detect this type of scan in Wireshark we can use filter "`tcp.flags==0X029` (Figure 6).

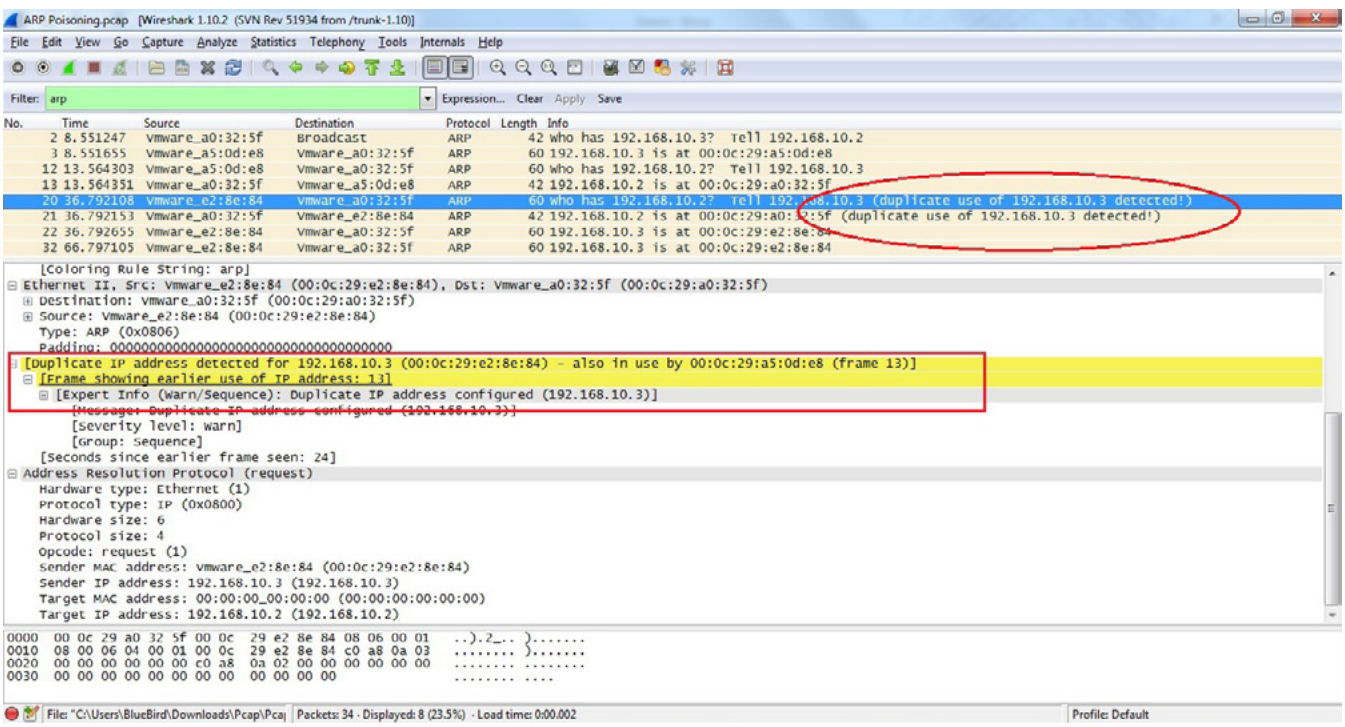

Figure 9. *ARP Poisioning*

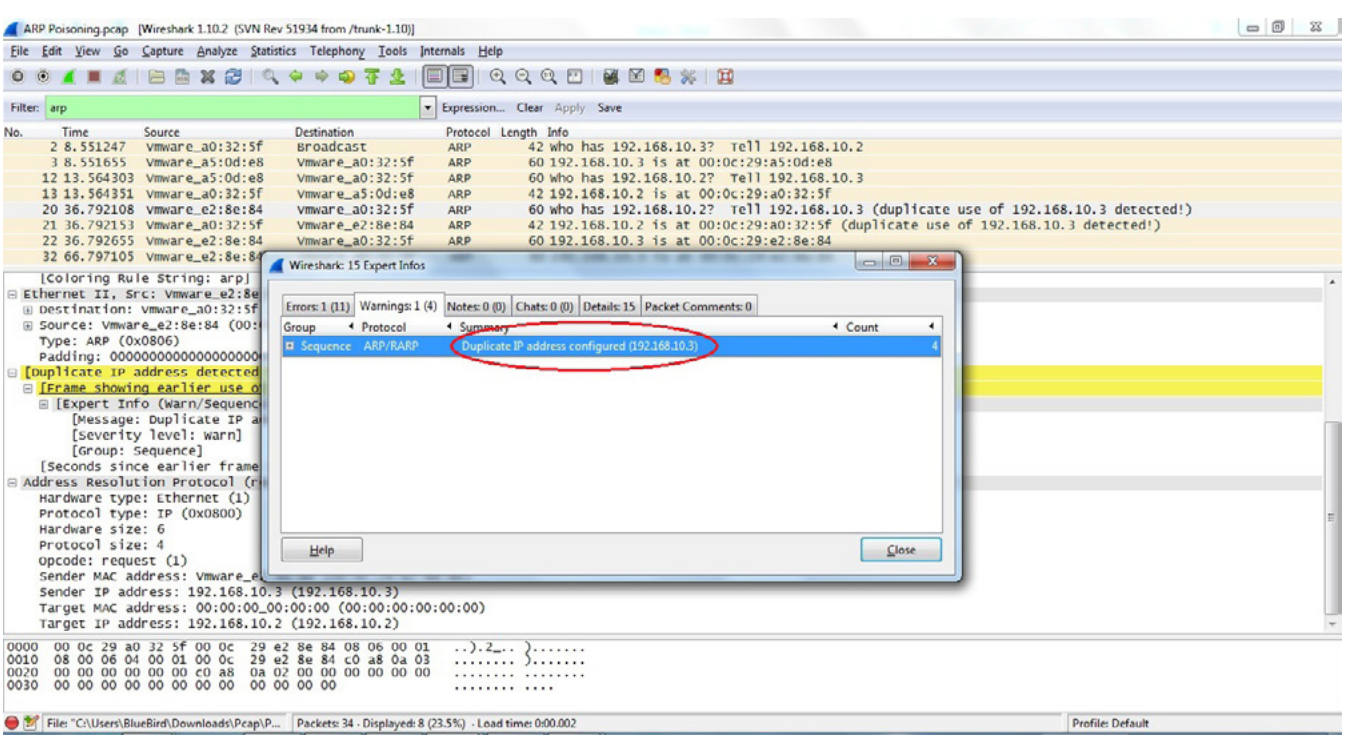

Figure 10. *ExpertInfo window*

UDP Scan

In UDP scan attacker sends a UDP packet (contains no meaningful data) on the target port and if that target responds with ICMP Type 3 Code 3 port is unavailable but if there is no response then it might be open or filtered. After capturing packets in Wireshark if you are getting high no. of packets with ICMP type 3 Code 3, it is a sign of UDP Scan. We can use filter `icmp.type==3 and icmp.code==3` to detect UDP scan in Wireshark.

IP Protocol Scan

IP Protocol Scan is helpful in finding out protocols running over IP. To detect this attacker sends packet with different protocol nos., if he gets ICMP type 3 Code 2 Packet as a response then it means that this protocol is not running on the target system while no response means protocol is there or filtered. To detect this scan in Wireshark, we can apply `icmp.type==3` and `icmp.code==2` as a filter (Figure 8).

ARP Poisoning

ARP poisoning is a layer 2 redirection technique which can be easily identified by Wireshark. If more than one MAC addresses claim to have the same IP address it will highlight that packet as *Duplicate IP Address Detected* (Figure 9).

If we find challenge in finding such packets, by reading packet details we can go to top menu Analyze -> ExpertInfo and then Warnings tab as shown in the picture (Figure 10). Here it will display all warning messages related to this capture which will help us to identify problems quickly.

Application Mapping

Wireshark can be used for application mapping as well, for example, if I am using HTTP communication then start looking for GET packet, within this packet if I will look for user-agent under Hypertext Transfer Protocol section it may reveal application OS and browser information (Figure 11). As we can see in the above picture that host is using Dropbox client tool version 2.0.22 on Windows 7 Operating System. I hope this article was useful and it will help you in understanding how Wireshark can be used to detect/analyze scanning traffic.

SANTOSH KUMAR

Santosh Kumar has more than 8 years of experience in IT Security. He is currently working as Technical Manager (IT Security) with Koenig Solutions Ltd. Santosh is proudly certified with Check Point Certified Managed Security Expert (CCMSE), Check Point Certified Security Expert (CCSE), CISCO ASA Specialist, Certified Ethical Hacker (CEH) along with many others. He also has proven track record of streamlining security processes, design and implement efficient security solutions, lead and assist multi-disciplined, multinational teams in achieving security efficiency.

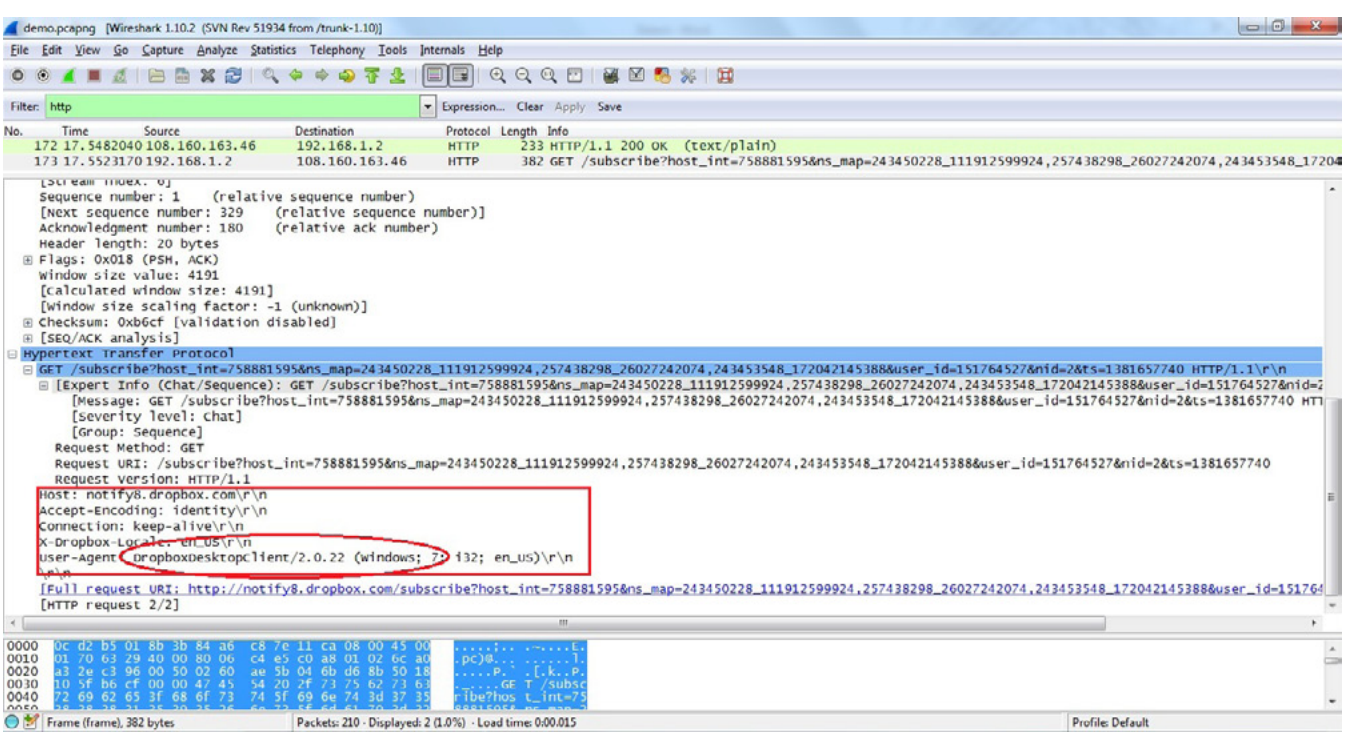

Figure 11. *Application Mapping*

KOENIG
WORLD'S #1 OFFSHORE TRAINING

Be Certified
& Expert in →

info@koenig-solutions.com www.koenig-solutions.com +91 88009 40444