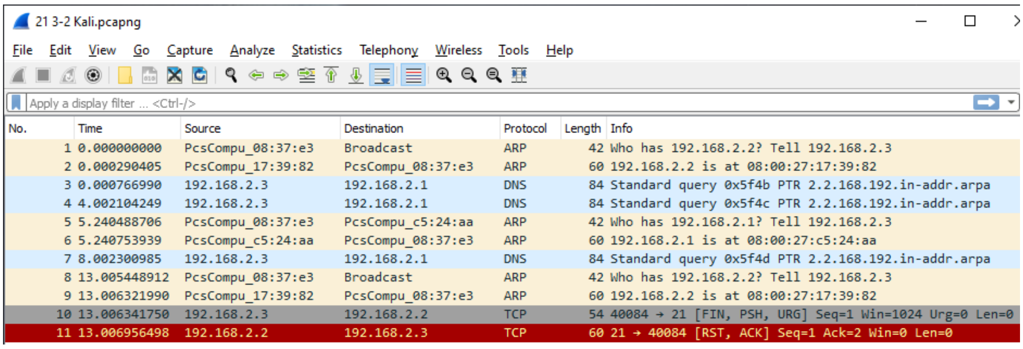
Justin Bland - 218478549
SIT379 - Task 3.2C – Week 3

Subtask 1

Place your one Kali VM and one XP VM on the same virtual network. Perform an XMAS scan on the XP machine, while capturing the packets between them. You should submit the following.

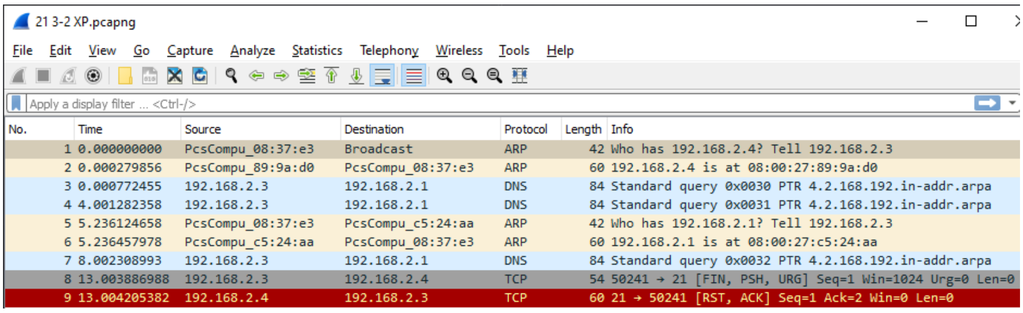
1. A short explanation of the differences you see in the XMAS scan against the Windows machine versus against what happened when scanning the Kali machine. Reference your packet capture in the explanation.

   In this task I have preformed an XMAS scan against both a Windows XP and Kali Linux machine, for simplicity I narrowed the scope down to port 21 on both machines to make analysing the data easier. With the kali machine in its default state and the windows machine with its firewall off both scans showed similar results with port 21 being closed and Wireshark shows a [RST,ACK] packet being returned.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_08:37:e3	Broadcast	ARP	42	Who has 192.168.2.2? Tell 192.168.2.3
2	0.000290405	PcsCompu_17:39:82	PcsCompu_08:37:e3	ARP	60	192.168.2.2 is at 08:00:27:17:39:82
3	0.000766990	192.168.2.3	192.168.2.1	DNS	84	Standard query 0x5f4b PTR 2.2.168.192.in-addr.arpa
4	4.002104249	192.168.2.3	192.168.2.1	DNS	84	Standard query 0x5f4c PTR 2.2.168.192.in-addr.arpa
5	5.240488706	PcsCompu_08:37:e3	PcsCompu_c5:24:aa	ARP	42	Who has 192.168.2.1? Tell 192.168.2.3
6	5.240753939	PcsCompu_c5:24:aa	PcsCompu_08:37:e3	ARP	60	192.168.2.1 is at 08:00:27:c5:24:aa
7	8.002300985	192.168.2.3	192.168.2.1	DNS	84	Standard query 0x5f4d PTR 2.2.168.192.in-addr.arpa
8	13.005448912	PcsCompu_08:37:e3	Broadcast	ARP	42	Who has 192.168.2.2? Tell 192.168.2.3
9	13.006321990	PcsCompu_17:39:82	PcsCompu_08:37:e3	ARP	60	192.168.2.2 is at 08:00:27:17:39:82
10	13.006341750	192.168.2.3	192.168.2.2	TCP	54	40084 → 21 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
11	13.006956498	192.168.2.2	192.168.2.3	TCP	60	21 → 40084 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

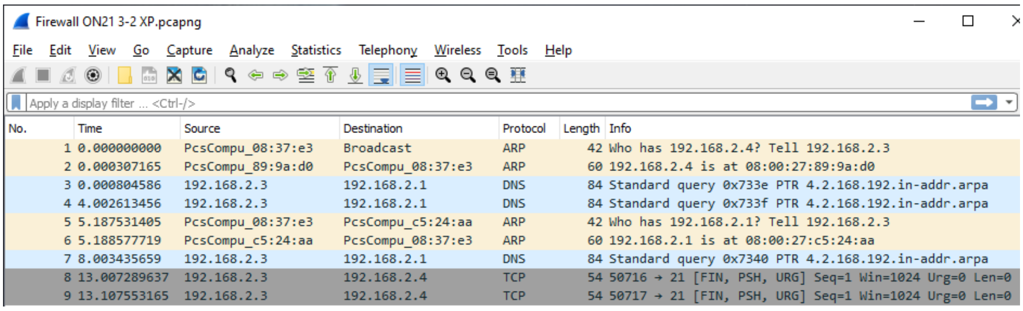
Kali Scan



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_08:37:e3	Broadcast	ARP	42	Who has 192.168.2.4? Tell 192.168.2.3
2	0.000279856	PcsCompu_89:9a:d0	PcsCompu_08:37:e3	ARP	60	192.168.2.4 is at 08:00:27:89:9a:d0
3	0.000772455	192.168.2.3	192.168.2.1	DNS	84	Standard query 0x0030 PTR 4.2.168.192.in-addr.arpa
4	4.001282358	192.168.2.3	192.168.2.1	DNS	84	Standard query 0x0031 PTR 4.2.168.192.in-addr.arpa
5	5.236124658	PcsCompu_08:37:e3	PcsCompu_c5:24:aa	ARP	42	Who has 192.168.2.1? Tell 192.168.2.3
6	5.236457978	PcsCompu_c5:24:aa	PcsCompu_08:37:e3	ARP	60	192.168.2.1 is at 08:00:27:c5:24:aa
7	8.002308993	192.168.2.3	192.168.2.1	DNS	84	Standard query 0x0032 PTR 4.2.168.192.in-addr.arpa
8	13.003886988	192.168.2.3	192.168.2.4	TCP	54	50241 → 21 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
9	13.004205382	192.168.2.4	192.168.2.3	TCP	60	21 → 50241 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

Windows XP Scan (Firewall OFF)

However, if I turn the windows firewall on like it would normally be the scan shows the port is in an "Open | Filtered" state along with Wireshark showing no packets being returned.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_08:37:e3	Broadcast	ARP	42	Who has 192.168.2.4? Tell 192.168.2.3
2	0.000307165	PcsCompu_89:9a:d0	PcsCompu_08:37:e3	ARP	60	192.168.2.4 is at 08:00:27:89:9a:d0
3	0.000804586	192.168.2.3	192.168.2.1	DNS	84	Standard query 0x733e PTR 4.2.168.192.in-addr.arpa
4	4.002613456	192.168.2.3	192.168.2.1	DNS	84	Standard query 0x733f PTR 4.2.168.192.in-addr.arpa
5	5.187531405	PcsCompu_08:37:e3	PcsCompu_c5:24:aa	ARP	42	Who has 192.168.2.1? Tell 192.168.2.3
6	5.188577719	PcsCompu_c5:24:aa	PcsCompu_08:37:e3	ARP	60	192.168.2.1 is at 08:00:27:c5:24:aa
7	8.003435659	192.168.2.3	192.168.2.1	DNS	84	Standard query 0x7340 PTR 4.2.168.192.in-addr.arpa
8	13.007289637	192.168.2.3	192.168.2.4	TCP	54	50716 → 21 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
9	13.107553165	192.168.2.3	192.168.2.4	TCP	54	50717 → 21 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

Windows XP Scan (Firewall ON)