

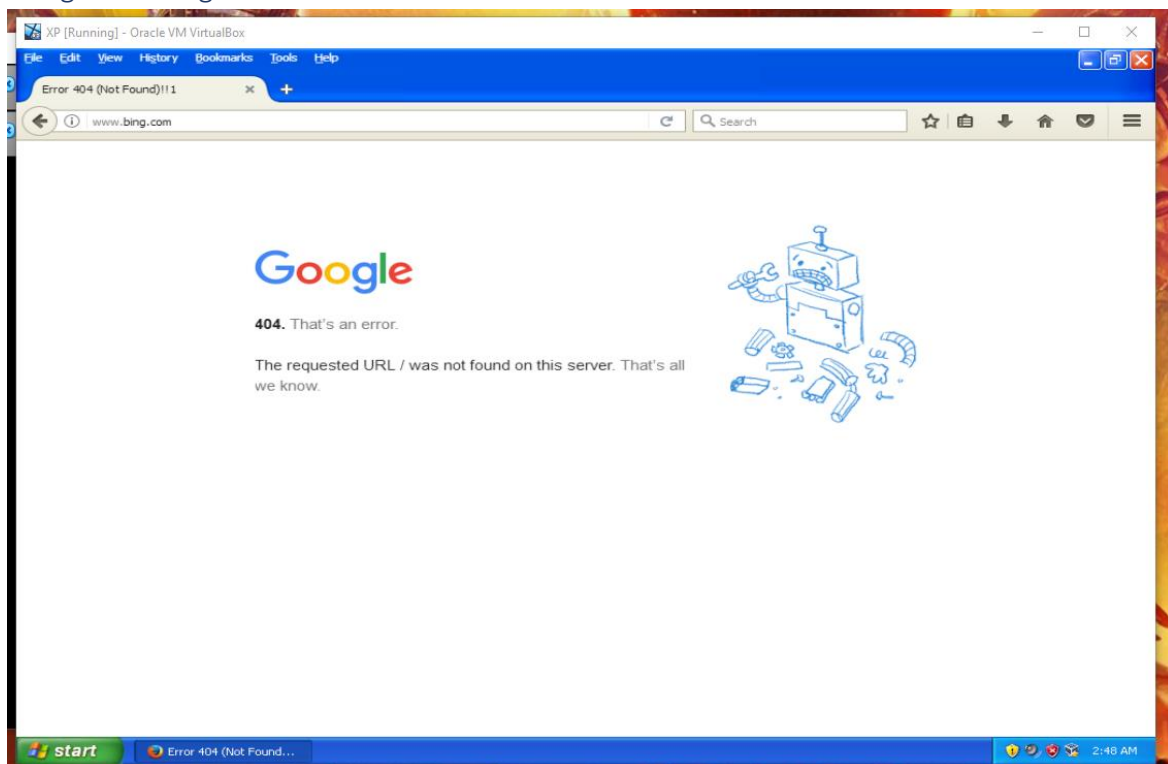
## Hijack DNS

### Subtask 1

Hijack a DNS query from your XP VM to PFSense. Capture the packets between your Kali attacker and your victim. You should submit the following.

1. A screenshot showing your victim receiving the wrong website when they attempt to navigate to bing.com
2. A screenshot of where in the packet capture the DNS hijacking is taking place.

1. A screenshot showing your victim receiving the wrong website when they attempt to navigate to bing.com



2. A screenshot of where in the packet capture the DNS hijacking is taking place.

Bing DNS spoof.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.109	192.168.1.1	DNS	72	Standard query 0x829e A www.bing.com
2	0.004135214	192.168.1.1	192.168.1.109	DNS	88	Standard query response 0x829e A www.bing.com A 142.250.66.206
3	0.005324900	192.168.1.109	192.168.1.1	DNS	72	Standard query 0x80ef AAAA www.bing.com
4	0.012101340	192.168.1.109	192.168.1.1	DNS	72	Standard query 0x80ef AAAA www.bing.com
5	0.017576838	192.168.1.109	142.250.66.206	TCP	62	1200 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	0.020165044	192.168.1.109	142.250.66.206	TCP	62	[TCP Out-Of-Order] 1200 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F
7	0.021313667	192.168.1.1	192.168.1.109	DNS	216	Standard query response 0x80ef AAAA www.bing.com CNAME a-0001.a-afdentry
8	0.028098216	192.168.1.1	192.168.1.109	DNS	216	Standard query response 0x80ef AAAA www.bing.com CNAME a-0001.a-afdentry
9	0.039746237	142.250.66.206	192.168.1.109	TCP	60	80 → 1200 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
10	0.044079400	142.250.66.206	192.168.1.109	TCP	58	[TCP Retransmission] 80 → 1200 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
11	0.044466785	192.168.1.109	142.250.66.206	TCP	60	1200 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
12	0.044748345	192.168.1.109	142.250.66.206	TCP	60	[TCP Dup ACK 11#1] 1200 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
13	0.045190947	192.168.1.109	142.250.66.206	HTTP	1085	GET / HTTP/1.1
14	0.052143564	192.168.1.109	142.250.66.206	TCP	54	1200 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
15	0.052306097	192.168.1.109	142.250.66.206	TCP	54	1200 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16	0.052453514	192.168.1.109	142.250.66.206	TCP	1085	[TCP Retransmission] 1200 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=1031
17	0.052805539	142.250.66.206	192.168.1.109	TCP	60	80 → 1200 [ACK] Seq=1 Ack=1032 Win=65535 Len=0
18	0.060213109	142.250.66.206	192.168.1.109	TCP	54	[TCP Dup ACK 17#1] 80 → 1200 [ACK] Seq=1 Ack=1032 Win=65535 Len=0
19	0.072401498	142.250.66.206	192.168.1.109	TCP	1514	80 → 1200 [ACK] Seq=1 Ack=1032 Win=65535 Len=1460 [TCP segment of a reas
20	0.072407567	142.250.66.206	192.168.1.109	HTTP	310	HTTP/1.1 404 Not Found (text/html)