Fragmentation Attacks

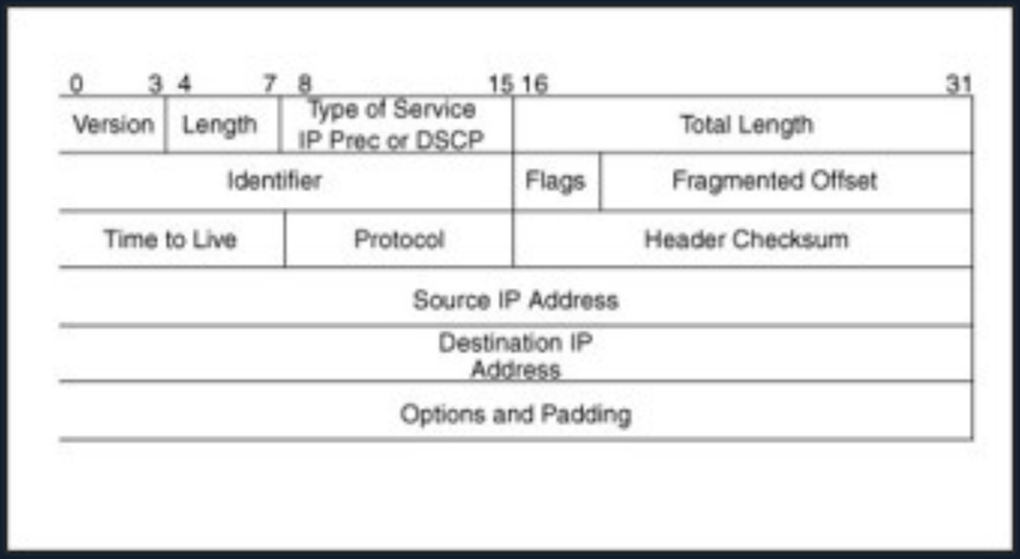
Related PCAP File(s):

- `nmap_frag_fw_bypass.pcapng`

When we begin to look for network anomalies, we should always consider the IP layer. Simply put, the IP layer functions in its ability to transfer packets from one hop to another. This layer uses source and destination IP addresses for inter-host communications. When we examine this traffic, we can identify the IP addresses as they exist within the IP header of the packet.

However, it is essential to note that this layer has no mechanisms to identify when packets are lost, dropped, or otherwise tampered with. Instead, we need to recognize that these mishaps are handled by the transport or application layers for this data. To dissect these packets, we can explore some of their fields:

1. `Length - IP header length`: This field contains the overall length of the IP header.
2. `Total Length - IP Datagram/Packet Length`: This field specifies the entire length of the IP packet, including any relevant data.
3. `Fragment Offset`: In many cases when a packet is large enough to be divided, the fragmentation offset will be set to provide instructions to reassemble the packet upon delivery to the destination host.
4. `Source and Destination IP Addresses`: These fields contain the origination (source) and destination IP addresses for the two communicating hosts.



Commonly Abused Fields

Innately, attackers might craft these packets to cause communication issues. Traditionally, an attacker might attempt to evade IDS controls through packet malformation or modification. As such, diving into each one of these fields and understanding how we can detect their misuse will equip us with the tools to succeed in our traffic analysis efforts.

Abuse of Fragmentation

Fragmentation serves as a means for our legitimate hosts to communicate large data sets to one another by splitting the packets and reassembling them upon delivery. This is commonly achieved through setting a maximum transmission

unit (MTU). The MTU is used as the standard to divide these large packets into equal sizes to accommodate the entire transmission. It is worth noting that the last packet will likely be smaller. This field gives instructions to the destination host on how it can reassemble these packets in logical order.

Commonly, attackers might abuse this field for the following purposes:

1. `IPS/IDS Evasion` - Let's say for instance that our intrusion detection controls do not reassemble fragmented packets. Well, for short, an attacker could split their nmap or other enumeration techniques to be fragmented, and as such it could bypass these controls and be reassembled at the destination.
2. `Firewall Evasion` - Through fragmentation, an attacker could likewise evade a firewall's controls through fragmentation. Once again, if the firewall does not reassemble these packets before delivery to the destination host, the attacker's enumeration attempt might succeed.
3. `Firewall/IPS/IDS Resource Exhaustion` - Suppose an attacker were to craft their attack to fragment packets to a very small MTU (10, 15, 20, and so on), the network control might not reassemble these packets due to resource constraints, and the attacker might succeed in their enumeration efforts.
4. `Denial of Service` - For old hosts, an attacker might utilize fragmentation to send IP packets exceeding 65535 bytes through ping or other commands. In doing so, the destination host will reassemble this malicious packet and experience countless different issues. As such, the resultant condition is successful denial-of-service from the attacker.

If our network mechanism were to perform correctly. It should do the following:

- `Delayed Reassembly` - `The IDS/IPS/Firewall should act the same as the destination host, in the sense that it waits for all fragments to arrive to reconstruct the transmission to perform packet inspection.`

Finding Irregularities in Fragment Offsets

In order to better understand the abovementioned mechanics, we can open the related traffic capture file in Wireshark.

Fragmentation Attacks

```
MisaelMacias@htb[/htb]$ wireshark nmap_frag_fw_bypass.pcapng
```

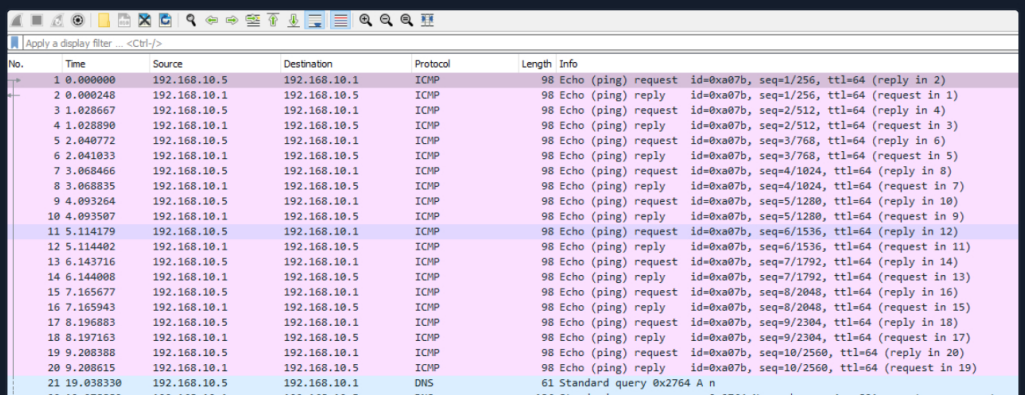
For starters, we might notice several ICMP requests going to one host from another, this is indicative of the starting requests from a traditional Nmap scan. This is the beginning of the host discovery process. An attacker might run a command like this.

Attacker's Enumeration

Fragmentation Attacks

```
MisaelMacias@htb[/htb]$ nmap <host ip>
```

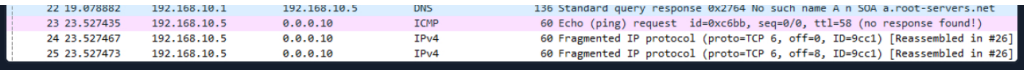
In doing so, they will generate the following.



OFFLINE

Start Instance

∞ / 1 spawns left



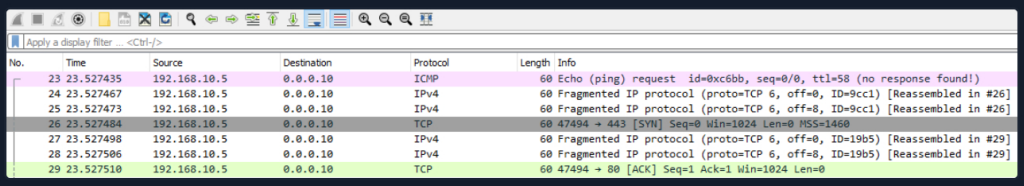
No.	Time	Source	Destination	Protocol	Length	Info
22	19.078882	192.168.10.1	192.168.10.5	DNS	136	Standard query response 0x2764 No such name A n SOA a.root-servers.net
23	23.527435	192.168.10.5	0.0.0.10	ICMP	60	Echo (ping) request id=0xc6bb, seq=0/0, ttl=58 (no response found!)
24	23.527467	192.168.10.5	0.0.0.10	IPv4	60	Fragmented IP protocol (proto=TCP 6, off=0, ID=9cc1) [Reassembled in #26]
25	23.527473	192.168.10.5	0.0.0.10	IPv4	60	Fragmented IP protocol (proto=TCP 6, off=8, ID=9cc1) [Reassembled in #26]

Secondarily, an attacker might define a maximum transmission unit size like this in order to fragment their port scanning packets.

Fragmentation Attacks

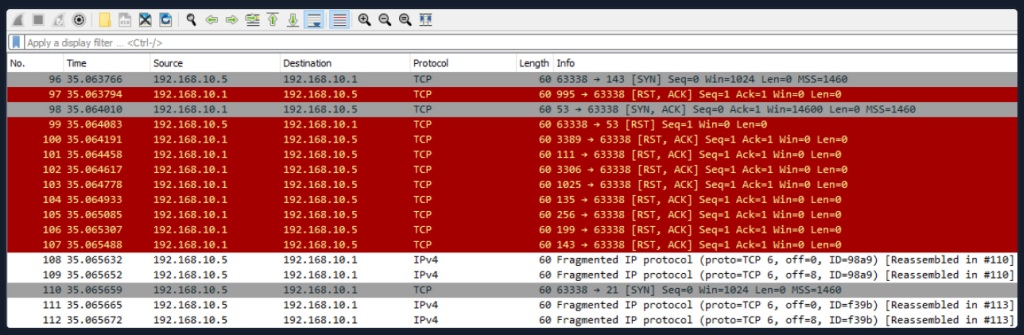
```
MisaelMacias@htb[/htb]$ nmap -f 10 <host ip>
```

In doing so they will generate IP packets with a maximum size of 10. Seeing a ton of fragmentation from a host can be an indicator of this attack, and it would look like the following.



No.	Time	Source	Destination	Protocol	Length	Info
23	23.527435	192.168.10.5	0.0.0.10	ICMP	60	Echo (ping) request id=0xc6bb, seq=0/0, ttl=58 (no response found!)
24	23.527467	192.168.10.5	0.0.0.10	IPv4	60	Fragmented IP protocol (proto=TCP 6, off=0, ID=9cc1) [Reassembled in #26]
25	23.527473	192.168.10.5	0.0.0.10	IPv4	60	Fragmented IP protocol (proto=TCP 6, off=8, ID=9cc1) [Reassembled in #26]
26	23.527484	192.168.10.5	0.0.0.10	TCP	60	47494 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	23.527498	192.168.10.5	0.0.0.10	IPv4	60	Fragmented IP protocol (proto=TCP 6, off=0, ID=19b5) [Reassembled in #29]
28	23.527506	192.168.10.5	0.0.0.10	IPv4	60	Fragmented IP protocol (proto=TCP 6, off=8, ID=19b5) [Reassembled in #29]
29	23.527510	192.168.10.5	0.0.0.10	TCP	60	47494 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0

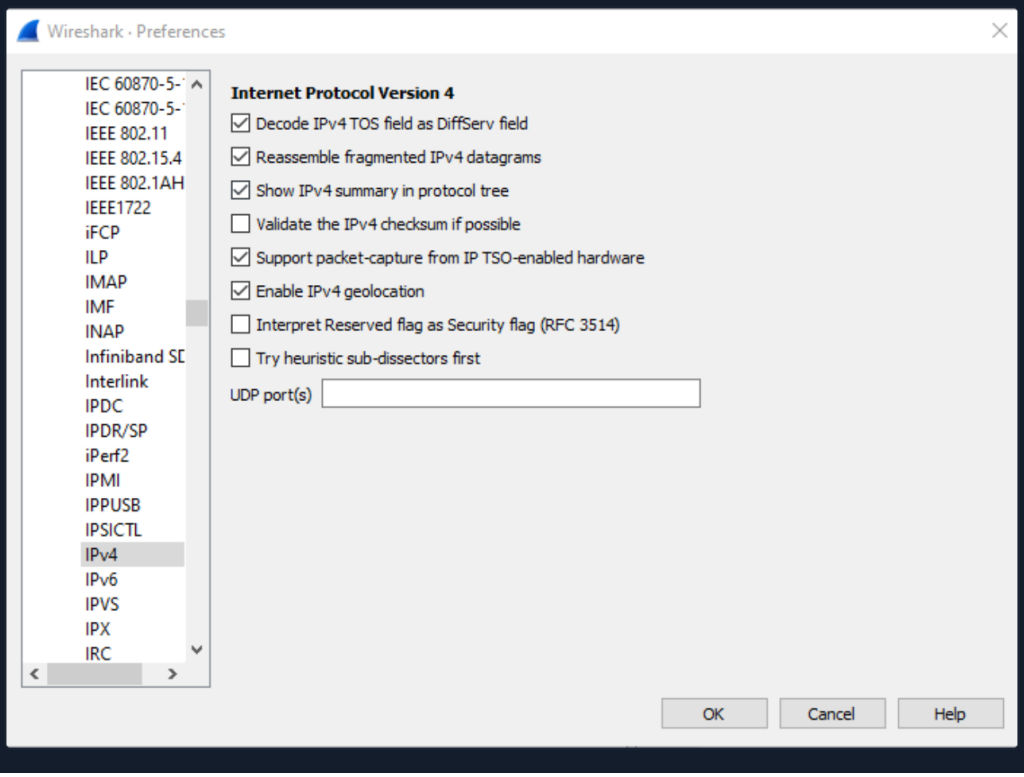
However, the more notable indicator of a fragmentation scan, regardless of its evasion use is the single host to many ports issues that it generates. Let's take the following for instance.



No.	Time	Source	Destination	Protocol	Length	Info
96	35.063766	192.168.10.5	192.168.10.1	TCP	60	63338 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
97	35.063794	192.168.10.1	192.168.10.5	TCP	60	995 → 63338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
98	35.064010	192.168.10.1	192.168.10.5	TCP	60	53 → 63338 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
99	35.064083	192.168.10.5	192.168.10.1	TCP	60	63338 → 53 [RST] Seq=1 Win=0 Len=0
100	35.064191	192.168.10.1	192.168.10.5	TCP	60	3389 → 63338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	35.064458	192.168.10.1	192.168.10.5	TCP	60	111 → 63338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
102	35.064617	192.168.10.1	192.168.10.5	TCP	60	3306 → 63338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
103	35.064778	192.168.10.1	192.168.10.5	TCP	60	1025 → 63338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	35.064933	192.168.10.1	192.168.10.5	TCP	60	135 → 63338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
105	35.065085	192.168.10.1	192.168.10.5	TCP	60	256 → 63338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	35.065307	192.168.10.1	192.168.10.5	TCP	60	199 → 63338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	35.065488	192.168.10.1	192.168.10.5	TCP	60	143 → 63338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
108	35.065632	192.168.10.5	192.168.10.1	IPv4	60	Fragmented IP protocol (proto=TCP 6, off=0, ID=98a9) [Reassembled in #110]
109	35.065652	192.168.10.5	192.168.10.1	IPv4	60	Fragmented IP protocol (proto=TCP 6, off=8, ID=98a9) [Reassembled in #110]
110	35.065659	192.168.10.5	192.168.10.1	TCP	60	63338 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
111	35.065665	192.168.10.5	192.168.10.1	IPv4	60	Fragmented IP protocol (proto=TCP 6, off=0, ID=f39b) [Reassembled in #113]
112	35.065672	192.168.10.5	192.168.10.1	IPv4	60	Fragmented IP protocol (proto=TCP 6, off=8, ID=f39b) [Reassembled in #113]

In this case, the destination host would respond with RST flags for ports which do not have an active service running on them (aka closed ports). This pattern is a clear indication of a fragmented scan.

If our Wireshark is not reassembling packets for our inspection, we can make a quick change in our preferences for the IPv4 protocol.



Connect to Pwnbox
Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 138ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

+ 1 Inspect the nmap_frag_fw_bypass.pcapng file, part of this module's resources, and enter the total count of packets that have the TCP RST flag set as your answer.

66535

Submit

Previous Next

Mark Complete & Next