حمله ICMP FLOOD یا PING FLOOD

نوعی از حملات DOS است که حمله‌کننده پیام های فراوانی از نوع پینگ (Ping) به قربانی ارسال می‌کند تا سرور را از کار بیندازد.

درICMP Flood Attack ، پیام‌ها از نوعping ، یعنی یکی از معروف‌ترین انواع پیام‌های پروتکل ICMP، هستند.

به همین دلیل به این حمله Ping Flood Attack نیز گفته می‌شود.

توجه کنید که اگر این پیام‌ها از مبداهای متفاوتی ارسال شوند، به آن حمله منع سرویس توزیع شده (DDoS)گفته می‌شود.

پیام Ping

برای بررسی برقرار بودن ارتباط بین دو دستگاه و همچنین محاسبه‌ی زمان رفت و برگشت یک بسته (packet)بین دو دستگاه، از این پیام استفاده می‌شود.

برای نمونه، دستگاه A که در آدرس IP=12.34.56.78 قرار دارد، برای بررسی ارتباط با دستگاه B که در آدرس IP = 10.11.12.13 قراردارد، یک پیام ping که مبدا و مقصد آن آدرس‌های بیان شده هستند، تولید و ارسال می‌کند.(ICMP-echo-request)

دستگاه B با دریافت این پیام (اگر ارتباط بین دو دستگاه برقرار باشد)، آن را پردازش و یک پیام ping با مبدا و مقصدی برعکس آن‌چه از پیام ping اول دریافت کرده است، تولید می‌کند و آن را برای دستگاه A می‌فرستد.(ICMP-echo-reply)

به این ترتیب، اگر A پاسخ B را دریافت کند، از صحت ارتباط خود با او مطمین و زمان رفت و برگشت پیام را نیز متوجه می‌شود.

عملکرد ICMP Flood Attack

از آن‌جایی که هر دستگاه ظرفیت مشخصی برای پاسخ به یک پیام دارد، در ICMP Flood Attack تعداد زیادی از این نوع پیام به سمت قربانی ارسال می‌شود تا ظرفیت پردازش و همچنین پهنای باند او تکمیل شود و نتواند به پیام‌های واقعی و ضروری خود پاسخ گوید.

حمله‌کننده به چند روش می‌تواند حمله را پیاده‌سازی کند:

1- در ساده‌ترین و ابتدایی‌ترین روش، حمله کننده با دستگاه خود پیام ping را به قربانی ارسال می‌کند.

این روش محدود به ظرفیت پردازشی و پهنای باند دستگاه حمله‌کننده است و از طرفی ظرفیت خود دستگاه نیز تلف می‌شود.

2- پیاده‌سازی ICMP Flood Attack ، حمله‌ای با نام Smurf attack

در این روش، حمله‌کننده بدون آن‌که هزینه‌ای برای در اختیار گرفتن تعدادی دستگاه بکند، از دستگاه‌های یک شبکه برای پیاده کردن حمله‌ی خود (به‌شکل رایگان) استفاده می‌کند.

فرض کنید حمله‌کننده پیام ping را به آدرس gateway یک شبکه‌ی دل‌خواه به‌شکل broadcast ارسال می‌کند. در این حالت، پیام او به‌وسیله‌ی gateway به تمامی دستگاه‌های موجود در شبکه ارسال می‌شود.

حمله کننده، IPارسال کننده‌ی ping را IP قربانی موردنظر خود قرار می‌دهد تا دستگاه‌های موجود در شبکه به جای آن‌که پاسخ ping را به خود حمله کننده ارسال کنند، پاسخ را با توجه به IP پیام ping دریافتی، به قربانی ارسال کنند.

بنابراین با ارسال تعداد مشخصی پیام ping به شبکه، چندین برابر آن تعداد، پیام به قربانی ارسال می‌شود و حمله‌کننده می‌تواند این کار را بدون صرف هزینه برای به دست آوردن دستگاه‌های واسطه انجام دهد.

3- روش دیگر، استفاده از تعدادی دستگاه (کامپیوتر) دیگر است که تحت فرمان و کنترل حمله‌کننده هستند) موسوم به.(botnet army)

در این نوع حمله، حمله‌کننده به این دستگاه‌ها دستور می‌دهد تا به یک آدرس مشخص، پیام ping ارسال کنند.

به این ترتیب، بدون درنظر گرفتن محدودیت‌های یک دستگاه، می‌توان با افزایش تعداد این دستگاه‌ها، حجم بالایی از پیام را به قربانی ارسال کرد.

توجه کنید که در این جا آدرس حمله‌کننده مخفی می‌ماند و به‌راحتی قابل شناسایی نیست.

البته امروزه به دلیل استفاده از firewall ، چنین شبکه‌های آسیب‌پذیری به ندرت یافت می‌شوند.

امیدواریم مقاله آشنایی با حملات سیل Ping مفید بوده باشد.