Syn-cookie

Arash Taherkalateh 882980

Syn-Cookie روشی که توسط ادمین سایت‌ها به کار گرفته میشود به منظور مقابل با حمله Syn-Flooding . این روش از حمله از پروسس شکل‌گیری ارتباط بین Client و Server ، که یک عملیات سه‌جانبه، معروف به Three-way Handshake است سوٗ استفاده می‌کند تا با ایجاد تعداد زیادی ارتباط باعث مشغول نگاه داشتن سرور (و یا Crash آن) شود. این روش‌ها هم اکنون دیگر چندان کاربردی نیست، به لطف تکنیک‌هایی مثل Syn-cookie .

در درجه اول لازم است بدانیم که این کوکی‌ها هیچ مشکل امنیتی متوجه Host یا Client نمیکنند و هدف آنها جلوگیری از ضایع شدن منابع سمت هاست است . این نوع از حملات بر مبنای اصول Tree-way Handshake کار می‌کند . به این صورت که اول Client یه درخواست اتصال به هاست میفرستد، که به این درخواست پیغام تطابقی یا SYN میگویند . هنگامی که هاست این پیغام را دریافت می‌کند، در جواب پیغام SYN-ACK را ارسال می‌کند . با ادامه پیدا کردن این روند در نهایت دو طرف به هم وصل میشوند. مشکلی که وجود دارد این است که معمولا سرورها صف کوچکی برای نگاه داری درخواست‌های SYN دارند، چیزی در حدود هشت تا در هر زمان .

یکی از روش‌های شناخته شده DoS attack که در بالا ذکر شد، با نام Syn-Flooding از همین واقعیت برای حمله استفاده می‌کند. تعداد زیادی پیغام SYN برای سرور ارسال میشود، سرور در جوان SYN-ACK میفرستد، اما پیغام ACK توسط Client ارسال نمی‌شود و این موضوع باعث میشود یکی از خانه‌های صف SYN مشغول بماند. چنانچه همه چیز درست پیش برود، تمام صف با این درخواست‌های بی جواب پر خواهد شد و سرور دیگر قادر به پاسخگویی به کاربر جدید نخواهد بود.

راه حل ارائه شده برای این نوع از حملات SYN-Cookie است . در اینجا چنین تظاهر میشود که هاست صفی بزرگتر از آنچه که واقعا دارد در اختیار دارد . در صورت رخداد حمله، یک SYN-ACK برای Client ارسال می‌کند، سپس با ساخت یک SYN-Cookie مرتبط با این درخواست ، SYN را از صف بیرون میرود. به این ترتیب این‌طور به نظر می‌رسد که اصلا درخواست SYN دریافت نشده است . هنگامی که پیغام SYN-ACK با SYN-Cookie توسط Client دریافت شد، حال میتواند جواب ACK متناسب را باتوجه به SYN-Cookie که اشاره گری به SYN-ACK اصلی است ارسال

کند . سرور میتواند از این داده‌ها برای ساخت SYN-ACK اولیه استفاده کند . حالا Client میتواند به هاست متصل شده و به رد و بدل داده بپردازد . در عین حال از مشغول شدن صف SYN هم جلوگیری شده است .