چگونه اکسس‌پوینت‌های جعلی را شناسایی کنیم؟

شبکه‌های بی‌سیم همواره در معرض تهدیدهای مختلف قرار دارند. در بیشتر موارد دسترسی به داده‌های شخصی هدف این مدل از حملات به شمار می‌روند. اما برای آن‌که بتوان یک تهدید را به یک حمله واقعی تبدیل کرد، لازم است تا کاربر فریب داده شود. این همان نقطه‌ای است که ابزار EvilAP_Defender به کمک مدیران شبکه آماده و به آن‌ها درباره وجود نقاط دسترسی (Access Points) غیرمجاز اطلاع‌رسانی می‌کند.

EvilAP_Defender یک ابزار منبع‌باز است که یک محدوده را برای نقاط دسترسی (Access Points) غیرمجاز (جعلی) بی‌سیم اسکن کرده و به مدیران شبکه درباره هر آن چیزی که پیدا کرده است، گزارش می‌دهد. به عبارت دقیق‌تر، این ابزار به طور ویژه برای شناسایی نقاط دسترسی به اصطلاح سرکش (Rough) کاربرد دارد که توسط هکرها برای تقلید و فریب کاربران استفاده قرار می‌گیرد. این نقاط دسترسی که به نام Evil Twins معروف هستند، به هکرها اجازه می‌دهند که ترافیک اینترنت را از دستگاه‌هایی که به آن متصل می‌شوند، ره‌گیری کنند. این کار برای سرقت هویت، کلاه‌برداری و مواردی از این دست می‌تواند مورد استفاده قرار گیرد. بیش‌تر کاربران، کامپیوترها و دستگاه‌های خود را به گونه‌ای پیکربندی می‌کنند که به طور خودکار به شبکه‌های بی‌سیم متصل شوند، شبیه به شبکه‌هایی که در خانه یا محل کار دارند.

زمانی‌که دو شبکه بی‌سیم با یک نام یا SSID یکسان وجود داشته باشند - که در بیشتر موارد آدرس MAC یا BSSID یکسانی نیز دارند- اکثر قریب به اتفاق این دستگاه‌ها به طور خودکار به شبکه‌ای که سیگنال قوی‌تری دارد، متصل می‌شوند. حملات Evil Twins درست در این نقطه به وقوع می‌پیوندند. زیرا هر دو SSID و BSSID ها می‌توانند جعل شوند. ابزار منبع‌باز EvilAP_Defender به زبان پایتون نوشته شده و روی گیت‌هاب منتشر شده است. این برنامه می‌تواند با استفاده از کارت شبکه بی‌سیم یک کامپیوتر نقاط دسترسی جعلی که یک نقطه دسترسی واقعی SSID و BSSID را تکرار کرده‌اند، کشف کند. همچنین، توانایی شناسایی موارد دیگری همچون کانال، رمز، پروتکل حریم خصوصی و احرازهویت را نیز دارد. محافظت از شبکه‌های بی‌سیم در فواصل زمانی منظم در برابر حملات Evil Twin از ویژگی‌های این ابزار به شمار می‌رود. این ابزار زمانی‌که برای اولین بار اجرا می‌شود، یا زمانی‌که همراه با سوییچ –L استفاده می‌شود، در وضعیت یادگیری (Learning) قرار خواهد گرفت، به طوری‌که اقدام به شناسایی شبکه‌های بی‌سیم در دسترس می‌کند. در ادامه فهرستی از شبکه‌های بی‌سیم پیدا شده درست کرده و آن‌ها را به رنگ سبز در یک فهرست سفید قرار می‌دهد. همچنین فهرستی از نقاط دسترسی و OUIها تهیه می‌کند. این ابزار همچنین یکسری تنظیمات در اختیار کاربر قرار می‌دهد که با استفاده از آن‌ها توانایی اضافه یا حذف SSIDها را به/از فهرست سفید خواهند داشت. در ادامه، مدیر با استفاده از سوییچ –N توانایی تغییر وضعیت از Learning به Normal (وضعیت عادی) را دارد. در این وضعیت ابزار شروع به اسکن نقاط دسترسی غیرمجاز می‌کند، اگر یک نقطه جعلی شناسایی شود، یک ایمیل هشداردهنده برای مدیر ارسال می‌شود، اما طراح در نظر دارد مکانیزمی را طراحی کند که در آینده این هشدارها از طریق پیام کوتاه نیز به مدیر اطلاع‌رسانی کنند. همچنین یک حالت پیش‌گیرانه در این ابزار وجود دارد، به این صورت که در زمان شناسایی نقاط دسترسی جعلی یک حمله منع سرویس DoS را روی این نقاط دسترسی مخرب انجام می‌دهد. در این حالت مدیران زمان کافی برای اتخاذ تدابیر دفاعی مناسب را خواهند داشت.

طراح این ابزار در مستنداتی که درباره این ابزار منتشر کرده است، می‌گوید: « حمله DoS فقط روی نقاط دسترسی جعلی که دارای SSID یکسانی بوده، اما از BSSID متفاوت یا کانال‌های متفاوتی استفاده می‌کنند، کاربرد دارد.» این‌کار برای پیشگیری از حمله به شبکه‌های مشروع و قانونی است. این ابزار توانایی شناسایی نقاط دسترسی جعلی زیر را دارد:

- نقطه دسترسی جعلی با یک آدرس BSSID متفاوت

- نقطه دسترسی جعلی درون یک BSSID یکسان با نقطه دسترسی قانونی اما با یک خصلت متفاوت

- نقطه دسترسی جعلی درون BSSID و خصلت (Attribute) یکسان و قانونی اما با پارامترهای برچسب‌گذاری شده متفاوت. پارامترهای برچسب‌گذاری شده مقادیر اضافی هستند که همراه با بیکون فریم beacon frame می‌آیند. (beacon frame در برگیرنده همه اطلاعات لازم درباره یک شبکه است. بیکن فریم‌ها از مؤلفه‌های؛ سرآیند مک، بدنه فریم و FCS تشکیل شده‌اند.)

البته حمله به نقاط دسترسی که در بیشتر موارد توسط هکرها انجام می‌شود، در بیش‌تر کشورها یک فرآیند غیرقانونی به حساب می‌آید.

اما برای استفاده از این نرم‌افزار لازم است برخی ملزومات را در اختیار داشته باشید. برای این‌که به توانید این ابزار را اجرا کنید، نیازمند بسته Aircrack-ng ، یک کارت شبکه بی‌سیم که از Aircrack-ng پشتیبانی کند، بانک اطلاعاتی MySQL و محیط زمان اجرای پایتون هستید.

تاریخ انتشار:

21 فروردین 1394

نشانی منبع: https://www.shabakeh-mag.com/security/517