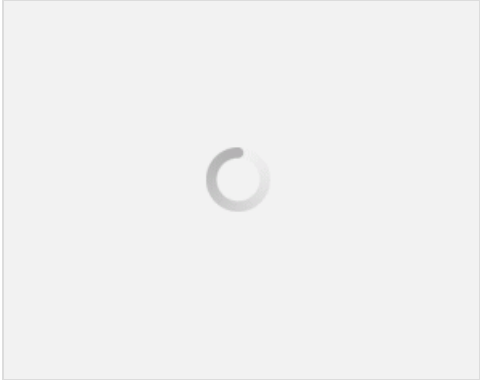
# جلوگیری از Rogue DHCP با استفاده از ابزار WISP میکروتیک (نسخه PDF)

Rogue DHCP سرور ها در واقع DHCP سـرور هایی هسـتند که یا بصورت مناسبی تنظیم نشـده اند و یا اینکه ناخواسـته یا بدون مجوز و بـدون اطلاع مـدیر شـبکه در شـبکه فعالیت میکنند . بیشتر اینگونه سـرور ها برای فعالیت های مخرب مورد اسـتفاده قرار می گیرند و در حملات مخرب به شبکه کاربر دارند. حتی اگر این سرور ها عملیات تخریبی انجام نداده و صرفا بصورت تصادفی در شبکه ایجاد شده باشند می توانند عملکرد سیستم ها و به ویژه کلاینت های شبکه را مختل کنند ، در صورت وجود چنین DHCP سرور هایی در شبکه کلاینت ها از این سـرویس استفاده کرده و تنظیمات IP دریافت می کننـد که مرتبط با شـبکه فعلی نبوده و یا تنظیمات نادرستی می باشـد ، برای مثال آدرس Gateway و یا DNS متفـاوتی با آنچه در محیط واقعی شـبکه وجود دارد دریافت می کننـد ، یک هکر می توانـد با راه انـدازی یک DHCP سـرور به این شکل خود را به عنوان سرویس دهنده به کلاینت معرفی کند و کلیه ترافیکی که توسط وی تولید می شود را مانیتور یا بهتر بگوییم Sniff کند. (اقتباس از مقاله مهندس نصیری)

برای درک این موضوع به سناریوی زیر دقت کنید:



شکل ۱ -WISP

در این سناریو ما یک WISP هستیم و قصد داریم مشترک های خود را طریق دو عدد AP به PPPOE Server متصل کنیم.

کلاینت ها از طریق Bridge به AP ها متصل هستند و از طریق کانکشن PPPOE در اکسس پوینت به اینترنت متصل میشن.

در حالت کلی هر کلاینت شبکه داخلی خود را دارد و از DHCP Server موجود در اکسس پوینت Ip می گیرد.

همانطور که می دانید ازتباط Bridge یک ارتباط لایه ۲ می باشد. Bridge نیز همانند Switch قادر است دو یا چند شبکه همنوع (Ethernet) را به هم پیونـد بزنـد و فریمها را بین انها مبادله نمایـد ، از این دیـدگاه فرقی با هم ندارند و متخصصـین شـبکه این دو را معادل یکدیگر میدانند. تنها نکته ای که Bridge را از Switch متمایز میکند آنست که Bridge می توانند دو شبکه غیر همنوع (مثل Wireless و Ethernet)را بهم متصل کرده و عملیات تغییر و تبدیل فریمها و نهایتا هدایت آنها را انجام بدهد.

برای درک بهتر موضوع ابتدا با نحوه عملکرد پروتکل DHCP آشنا می شویم.

شکل ۲ – DHCP operation

عملکرد DHCP به چهار قسمت پایه تقسیم می‌گردد:

- اکتشاف (DHCP Discovery)
- پیشنهاد (DHCP Offer)
- درخواست (DHCP Request)
- تصدیق (DHCP Acknowledgement)

این چهار مرحله به صورت خلاصه با عنوان DORA شناخته می‌شوند که هر یک از حرف‌ها، سرحرف مراحل بالا می‌باشد.

DHCP Discovery (اکتشاف DHCP)

هر سـرویس گیرنده (کاربر) برای شـناسایی سرورهای DHCP موجود اقدام به فرسـتادن پیامی در زیر شـبکه خود می‌کند. مدیرهای شـبکه می‌تواننـد مسـیریاب محلی را به گونه ایی پیکربنـدی کنند که بتواند بسـته داده‌ای DHCP را به یک سـرور DHCP دیگر که در زیر شـبکه متفاوتی وجود دارد، بفرستد. این مهم باعث ایجاد بسته داده با پروتکل UDP می‌شود که آدرس مقصد ارسالی آن ۲۵۵/۲۵۵/۲۵۵/۲۵۵ و یا آدرس مشـخص ارسال زیر شـبکه می‌باشد. کاربر (سـرویس گیرنده) DHCP همچنین می‌توانـد آخرین آی پی آدرس شـناخته شـده خود را درخواست بدهد. اگر سـرویس گیرنده همچنان به شـبکه متصل باشد در این صورت آی پی آدرس معتبر می‌باشد و سـرور ممکن است که درخواست را بپذیرد. در غیر اینصورت، این امر بستگی به این دارد که سرور به عنوان یک مرجع معتبر باشد. یک سرور به عنوان یک مرجع معتبر درخواست فوق را نمی‌پذیرد و سـرویس گیرنده را مجبور می‌کند تا برای درخواست آی پی جدید عمل کند. یک سـرور به عنوان یک مرجع غیرمعتبر به سادگی درخواست را نمی‌پـذیرد و آن را به مثابهی یک درخواست پیاده‌سازی از دست رفته تلقی می‌کنـد؛ و از سـرویس گیرنده می‌خواهد درخواست را لغو و یک آی پی آدرس جدید درخواست کند.

**DHCP Offer (پیشنهاد DHCP)**

زمانی که یک سـرور DHCP یک درخواست را از سـرویس گیرنـده (کاربر) دریافت می‌کنـد، یک آی پی آدرس را برای سـرویس گیرنـده رزو می‌کنـد و آن را بـا نام DHCP Offer برای کـاربر می‌فرسـتد. این پیام شامل: MAC آدرس (آدرس فیزیکی دسـتگاه) کـاربر؛ آی پی آدرسـی پیشنهادی توسط سرور؛ Subnet Mask آی پی؛ زمان تخصیص آی پی (lease Duration) و آی پی آدرس سروری می‌باشد که پیشنهاد را داده است.

**DHCP Request (درخواست DHCP)**

سرویس گیرنـده با یک درخواست به مرحله پیشـین پاسـخ می‌گویـد. یک کاربر می‌تواند پیشـنهادهای‌های مختلفی از سـرورهای متفاوت دریـافت کنـد. امـا فقـط می‌توانـد یکی از پیشـنهادها را بپـذیرد. بر اسـاس تنظیمـات شـناسایی سـرور در درخواست و فرسـتادن پیـام‌ها (identification option)، سـرورها مطلع می‌شوند که پیشـنهاد کدام یک پذیرفته شده است. هنگامی که سـرورهای DHCP دیگر این پیام را دریافت می‌کنند، آن‌ها پیشـنهادهای دیگر را، که ممکن است به کاربر فرستاده باشند، باز پس می‌گیرند و آن‌ها را در مجموعه آی پی‌های در دسترس قرار می‌دهند.

**DHCP Acknowledgement (تصدیق DHCP)**

هنگامی که سرور DHCP، پیام درخواست DHCP را دریافت می‌کند، مراحل پیکربندی به فاز پایانی می‌رسد. مرحله تصدیق شامل فرسـتادن یک بسته داده‌ای (DHCP Pack) به کاربر می‌باشـد. این داده بسـته ای شامل: زمان تخصـیص آی پی و یا هرگونه اطلاعات پیکربندی که ممکن بوده است که سرویس گیرنده درخواست کرده باشد، می‌باشد. در این مرحله فرایند پیکربندی آی پی کامل شده است.

حال تصور کنید که ما یک DHCP Server در روی اینترفیس Bridge یکی از رادیو های کلاینت قرار بدیم. چه اتفاقی میافتد؟

به تصویر زیر دقت کنید:

شکل ۳ – DHCP Offer

یکت DHCP Offer از ذوی بستر Bridge عبور می کنـد و به مقصد همه ی کلاینت های روی هر دو AP ارسال می شود و هر Node در شبکه که روی DHCP Client تنظیم شـده باشـد و این پکت را دریافت کند به آن پاسخ می شدهد و یک DHCP Request به به سمت آن DHCP Server ارسال می کند.

شکل ۴ - DHCP Request

DHCP Server در پاسخ یک پکت DHCP ACK ارسال می کند که حاوی IP , Gateway , DNS و ... می باشد.

شکل ۵ – DHCP ACK

با تعیین IP Address , DNS , Gateway می توان گفت که شبکه ما مختل شده است. به این می گویند Roge DHCP که خواسته یا ناخواسته توسط کلاینت ها در شبکه و عدم دقت کافی در کانفیگ AP ها توسط WISP ها بوجود می آید.

**اکنون برای جلوگیری از این مشکل چه باید کرد:**

۱- جلوگیری از ارتباط کلاینت های یک AP با سایر کلاینت های همان AP

برای این کار وارد تنظیمات کارت شبکه AP می شویم و مراحل زیر را انجام می دهیم

گزینه Defualt Forward را غیر فعال می کنیم

شکل ۵ – AP Config

شکل ۵ – AP Config

اگر مراحل فوق را به درستی طی کرده باشد نتیجتا دیگر کلاینت های روی این AP نمی توانند با یکدیگر ارتباط برقرار کنند.

۲- جلوگیری از ارتباط کلاینت های AP۱ با کلاینت های AP۲

این کار به دو روش امکان پذیر است:

a. جدا کردن Broadcast هر AP توسط Vlan

در این روش ما AP ها را بوسیله یک Management Switch به PPPOE Server متصل می کنیم و هر کدام از پورت های Switch که AP ها به آنها متصل هستند را در یک Broadcact منحصر به فرد قرار می دهیم. با این کار مشترک های هر AP را از سایر AP ها جدا میکنیم و کلاینت ها دیگر نمی توانند به کلاینت های سایر AP ها پکت ارسال کنند.

b. با استفاده از Bridge Filter Rule

به این نکته دقت کنید که ما سرویس اینترنت را بصورت PPPOE به کلاینت ها عرضه می کنیم پس ضرورتی ندارد که پروتکل های دیگری بغیر از PPPOE از بستر Bridge ما عبور کنند. برای جلوگیری از عبور سایر پروتکل کد های زیر را در ترمینال روتر کپی می کنیم:

```
interface bridge filter/

\ add action=accept chain=forward in-interface=wlan\ in-interface-list=all

mac-protocol=pppoe-discovery

\ add action=accept chain=forward in-interface=wlan\ in-interface-list=all

mac-protocol=pppoe

add action=drop chain=forward in-interface=wlan\ in-interface-list=all
```

و یا مراحل زیر را انجام می دهیم:

اگر مراحل فوق را به درستی انجام داده باشید دیگر هیچ کلاینتی نمی تواند به AP ها پروتکلی غیر از PPPOE ارسال کند.

سربلند و سر به زیر باشید

مهندس عزیزاله بندزن

ذکر بدون نام منبع اشکال شرعی دارد

مطلب اصلی