۱۰۰ نکته آموزش کریو کنترل قسمت ۴۱ : تنظیمات IPS (نسخه PDF)

پیکربندی سرویس Intrusion Prevention

کریو کنترل سرویس یکپارچه(https:////www.snort.org) Snort است ، یک پیشگیرانه و سیستم محافظتی (IDS//IPS) تا شبکه محلی را به شبکه های معلوم و مشخص متصل کند . پیشگیری از یک نفوذ به شبکه و روش شناسایی این نفوذ می تواند به ما کمک کند تا با استفاده از رول های فایروال کریو کنترل مدیریت امنی بر روی ترافیک داشته باشیم . یکی از این حملات را می توان مثلا DDOS که حملات تکذیب سرویس است عنوان کرد که ترافیک بالایی را از طریق پورتی به سمت شبکه سرازیر می کنند و منابع سیستمی که کاربران با آن در تماس هستند را مختل می کنند .

- نکته : سیستم پیشگیری نفوذ کریو کنترل بر روی تمامی اینترفیس ها کنترل دارد و در گروه Internet interfaces کنترل و بلاک کردن ترافیک های ناشناس در اینترنت را انجام می دهد این سرویس روی شبکه های محلی و VPN کلاینت کارایی ندارد

تنظیمات Intrusion Prevention در کریو کنترل

۱- وارد بخش administration interface و بروید به Intrusion Prevention

۲- فعال سازی Enable Intrusion Prevention

۳- حالا مد هایی که در اینجا مدنظر دارید را انتخاب کنید (این مراحل سه مرحله دارد) :

- High severity : در برابر حملات و نفوذ های سطح بالا نظیر تروجان ها کارایی دارد
- Medium severity : فعالیت های مشکوک را زیر نظر می گیرد مثلاـ ترافیکی از طرف یک پروتکل غیر استاندارد که روی پروتکل استاندرد دیگری در جریان است
- Low severity : حملاتی که تهدید جدی محسوب نمی شوند مانند Port scan ها

۴- کلیک بر روی On the Kerio website, you can test these settings برای تست سیستم Intrusion Prevention برای هر دو IPv۴ و IPv۶ ، و همچنین ۳ نوع حمله به صورت Fake در هر سه مرحله high, middle, low severity ارسال و روی فایروال ازمایش می شود

۵- Apply کنید

- نکته : می توانید با Security log گزارشی از بلاک شدن و شناسایی نفوذ در فایروال را بررسی کنید

تنظیمات برای نادیده گرفتن نفوذ

چنانچه تنظیمات پیشگیری از نفوذ بر روی فایروال اثر معکوسی بدهد و آن دسته از ترافیکی که استاندارد است و به مشکل بلاک شدن بخورد :

۱- در بخش administration interface بروید به Security log

۲- این لاگ به طور مثال به صورت :

```
"IPS: Alert, severity: Medium, Rule ID: 1:2009700 ET VOIP
Multiple Unauthorized SIP Responses"
```

۳- ID number رول را کپی کنید

۴- در administration interface بروید به Intrusion Prevention

۵- کلیک Advanced

۶- در Advanced Intrusion Prevention Settings کلیک کنید Add

۷- کلیک ok و Apply

ترافیک مشروع حالا اجازه عبور دارد

مطلب اصلی