سرورهای VoIP که بروی اینترنت قرار می گیرند باید موارد امنیتی را رعایت کنند تا از هک شدن و قبض های میلیونی تلفن جلوگیری کنند.در این آموزش مواردی عنوان می شود که کاربردی بوده اما باید توجه داشت که امنیت هیچگاه صدرصدی نبوده ولی می توان از ضررهای بزرگ تا حدودی جلوگیری کرد.

نکات امنیتی:

پسوردها

- تغییر کلیه پسوردهای پیش فرض سرور
- پسوردهای داخلی ها
- پسورد های قوی برای داخلی ها و وب ایزابل
- قوی بودن پسورد شامل طولانی بودن پسورد
- شامل حروف بزرگ و کوچک و اعداد
- شامل علائم مانند $ % * @# و...
- محدود کردن رجیستر شدن داخلی ها فقط به یک IP مشخص

بستن دوصفر

- در صورتی که تماس های خارج از کشور ندارید بهترین کار برای جلوگیری از قبض های میلیونی مخابرات بستن دوصفر از سمت مخابرات است.
- همینطور می توانید بستن دوصفر را از سمت سرور VoIP با ماژول custom context در الستیکس و ماژول Class of service در ایزابل انجام دهید.

تنظیم مجدد ssh

یکی از راه های هک شدن سرور از طریق ssh است.نکات زیر برای ssh باید لحاظ شود:

- پسورد قوی
- تغییر پورت پیش فرض ssh
- فعال سازی محدودیت تعداد لاگین ناموفق

ماژول fail2ban

فعال سازی و تنظیم ماژول fail2ban که بسیار کاربردی است.

تنظیم AMI

در صورتی که ami بدرستی پیکربندی نشده باشد.هکرها با استفاده از ami تماس های خودکار زیادی با سرور شما انجام می دهند باید پسورد پیش فرض را تغییر داده و دسترسی به آن را محدود کرد.

TLS و SRTP

با استفاده از TLS و SRTP می توانید سیگنالینگ و مدیا را امن کنید.

برای اطلاعات بیشتر با شماره 02691002326 در تماس باشید.