باسمه تعالی

هشدار افزایش تعداد حملات Brute Force علیه سرویس‌دهنده‌های SSH در سطح کشور

مشاهدات میدانی نشان‌دهنده افزایش تعداد حملات Brute Force علیه سرویس‌دهنده‌های SSH در سطح کشور است. از این‌رو در مستند حاضر تعدادی از مهمترین روش‌های مقاوم‌سازی این سرویس‌دهنده در برابر این‌گونه از حملات بیان شده است.

با توجه به تعدد نسخه‌های SSH پیاده‌سازی شده، در این مستند تنها به نحوه مقاوم‌سازی سرویس‌دهنده OpenSSH به‌کار گرفته شده در Ubuntu 16.04 LTS پرداخته شده است[1]. بدیهی است که رئوس مطالب بیان شده برای تجهیزات مختلف صادق بوده ولی نحوه اجرای آن در هر تجهیز متفاوت است.

۱. غیرفعال‌سازی دسترسی کاربر ریشه

بایستی دسترسی کاربر root به ssh را غیرفعال نمود. برای این منظور باید خط دستور PermitRootLogin yes را در فایل پیکربندی پیدا کرده و آن را به PermitRootLogin no تغییر داد. سپس بایستی کاربری به‌جز root تعریف نمود و وی را مجاز به استفاده از ssh نمود.

۲. تغییر شماره پورت پیش‌فرض

یکی از راه‌های افزایش امنیت SSH ، تغییر شماره پورت پیش‌فرض آن است. پروتکل SSH به‌طور پیش فرض از پروتکل TCP و شماره پورت ۲۲ استفاده می‌کند. با تغییر شماره پورت پیش‌فرض می‌توان از انجام بعضی حملات کور و سطح پایین در امان ماند. در فایل پیکربندی می‌توان در خط دستور Port 22 شماره پورت را به شماره پورت دلخواه تغییر داد.

[1] فایل تنظیمات Open SSH در اوبونتو در مسیر /etc/ssh/sshd_config قرار دارد. برای ایجاد تغییرات در این فایل به سطح دسترسی ریشه نیاز است. توصیه می‌شود همواره قبل از انجام هرگونه تغییر در پیکربندی، از پیکربندی‌های قبلی یک نسخه پشتیبان تهیه شود تا در صورت بروز مشکل بتوان آن را برطرف نمود.

۳. استفاده از روش لاگین مبتنی بر کلید عمومی SSH

بهتر است به‌جای استفاده از روش مرسوم احراز اصالت توسط نام و کلمه عبور (که مستعد حمله جستجوی کامل است)، از روش احراز اصالت مبتنی بر کلید عمومی استفاده نمود. برای تولید زوج کلید برای رمزنگاری غیرمتقارن از دستور ssh-keygen -t key_type -b bits -C "comment" استفاده می‌شود (**بر روی ماشین کلاینت**). پس از اجرای این دستور یک سوال برای حفاظت از کلید پرسیده می‌شود که می‌تواند خالی گذاشته شود؛ ولی توصیه می‌شود که به آن پاسخ داده شود (کلید خصوصی SSH که برای آن عبارتی برای محافظت قرار داده نشده می‌تواند توسط هر کسی که مالکیت آن را ندارد نیز مورد استفاده قرار گیرد). سپس کاربر می‌تواند با استفاده از دستور ssh-copy-id کلید عمومی خود را به سرور منتقل نماید (برای مثال برای ارسال کلید عمومی نام کاربری APA به سروری با آدرس 192.168.1.1 از دستور ssh-copy-id APA@192.168.1.1 استفاده می‌شود).

از این پس کاربری که کلید خصوصی مناسبی در اختیار دارد، برای ورود به سرور دستور ssh APA@192.168.1.1 را وارد نموده و به سوال مربوط به کلید پاسخ می‌دهد و دیگر نیازی به وارد نمودن کلمه عبور نخواهد داشت.

۴. غیر فعال نمودن روش احراز اصالت توسط کلمه عبور

پس از پیکربندی روش احراز اصالت مبتنی بر کلید عمومی SSH و تست عملکرد صحیح آن، بایستی روش احراز اصالت توسط کلمه عبور را غیرفعال نمود. برای این منظور کافی است تا در سطر فایل پیکربندی PasswordAuthentication yes مقدار Yes را به no تغییر داد.

۵. تغییر پروتکل‌ها و الگوریتم‌های رمزنگاری پیش‌فرض

بر اساس آخرین توصیه‌نامه‌ها، بایستی حداقل از پروتکل‌ها و الگوریتم‌های رمزنگاری زیر با طول کلید مشخص شده (یا قوی‌تر) استفاده شود:

Ciphers: chacha20-poly1305, aes256-gcm, aes128-gcm, aes256-ctr, aes192-ctr, aes128-ctr
MACs: hmac-sha2-512-etm, hmac-sha2-256-etm, umac-128-etm

۶. تعریف لیست سفید کاربران

توصیه می‌شود تا لیست کاربرانی که امکان ورود به سیستم از طریق SSH دارند را محدود نمود (با استفاده از سطر AllowUsers در فایل پیکربندی). لیست سفید مجموعه کاربرانی هستند که اجازه ورود به سیستم از طریق پروتکل SSH را دارند. هر کاربر دیگری که در این لیست نباشد اجازه ورود از طریق SSH را ندارد.

۷. تعریف لیست سفید آدرس‌ها

توصیه می‌شود تا لیست آدرس‌های IP که امکان ورود به سیستم از طریق SSH دارند را مشخص نمود (با استفاده از سطر ListenAddress در فایل پیکربندی).

۸. قطع نمودن جلسات بیکار[۲]

جلسات بیکار می‌توانند خطرناک باشند. برای جلوگیری از تهدیدات احتمالی مرتبط با این امر می‌توان افراد را پس از آن‌که مدتی با سیستم کار نکردند، از سیستم خارج نمود. متغیر ClientAliveInterval میزان زمان برحسب ثانیه را مشخص می‌نماید و اگر در طول این مدت پیامی از سمت کاربر دریافت نشد، یک پیام در دسترس بودن به کاربر ارسال می‌شود. همچنین متغیر ClientAliveCountMax بیشترین تعداد دفعاتی را مشخص می‌کند که این پیام به کاربر فرستاده می‌شود. پس از این تعداد اگر پاسخی دریافت نشد، ارتباط کاربر ملغی می‌شود. در مثال زیر سرور هر ۵ دقیقه (۳۰۰ ثانیه) پیام در دسترس بودن برای کاربر ارسال می‌نماید. اگر بعد از دو بار پاسخی دریافت ننمود، کاربر را از سیستم خارج می‌کند:

```
ClientAliveInterval 300
ClientAliveCountMax 2
```

۹. انتخاب کلمه عبور پیچیده

برای جلوگیری از موفقیت حملات دیکشنری و جستجوی کامل بایستی درصورت استفاده از روش احراز اصالت مبتنی بر کلمه عبور، از پیچیدگی کلمات عبور اطمینان حاصل نمود.

---

[۲] Idle sessions