[illegible] CEH (Certified Ethical Hacker): [illegible]

[illegible]

[illegible] CEH [illegible].

[illegible] (Man-in-the-middle attack) [illegible] MITM [illegible].

[illegible].

Interlock

(SSL)

Hash

Carry-forward

بهطور کلی، درستی کلیدهای عمومی را باید از طریق روشی مطمئن شد، اما احتیاج به محرمانه بودن کلید ندارند . گذرواژهها و کلیدهای رمز بهاشتراک گذاشته شده، نیازهای محرمانگی بیشتری را طلب میکنند . کلیدهای عمومی به وسیله یک مرکز تأیید گواهی که کلید عمومی آن از طریق یک کانال امن (برای نمونه، توسط یک مرورگر وب یا یک برنامه نصب شده سامانهای) توزیع شده بررسی میشوند . کلیدهای عمومی نیز میتوانند از طریق یک وبگاه مورد اعتماد که کلید عمومی آن از طریق یک کانال امن (برای نمونه با جلسات چهره به چهره) توزیع شده، تأیید بشوند . برای طبقهبندی پروتکلهایی که با استفاده از شکلهای گوناگون کلید و گذرواژه از حملات مرد میانی جلوگیری میکنند باید به پروتکل تبادل کلید نگاه کرد .

تجزیه و تحلیل قانونی حمله مرد میانی

برای آگاه شدن از این موضوع که واقعاً حمله مرد میانی رخ داده یا خیر، میتوان ترافیک شبکه مصرف شده را تجزیه و تحلیل کرد . شواهد مهم برای تجزیه و تحلیل شبکه توسط افراد مظنون به حمله مرد میانی در امنیت لایه انتقال (SSL) به شرح زیر هستند :

- آدرس IP سرور (رایانه)
- نام سامانه نام دامنه سرور
- استاندارد اکس۵۰۹ سرور
  - آیا گواهی امضاء شدهاست؟
  - آیا گواهی توسط یک CA مورد اعتماد امضاء شدهاست؟
  - آیا گواهی باطل شدهاست؟
  - آیا گواهی به تازگی تغییر کردهاست؟
  - آیا کاربران دیگر، در جای دیگر محیط اینترنت، گواهی مشابهی را اخذ کردهاند؟

رمزنگاری کوانتومی

پروتکلهای رمزنگاری کوانتومی بهطور معمول همه یا بخشی از ارتباطات کلاسیک خود را با یک رویه احراز هویت ایمن و بیقید و شرط، احراز هویت میکنند که نمونه آن احراز هویت Wegman-Carter است.

فراتر از رمزنگاری

حمله مرد میانی باید به عنوان مشکلی کلی که ناشی از حضور عناصر واسطه به عنوان نماینده کاربران هر دو طرف است، دیده شود. اگر آنها دارای صلاحیت و قابل اعتماد باشند همه چیز ممکن است خوب باشد . اما اگر آنها دارای این ویژگیها نباشند هیچ چیز خوب نخواهد بود . حمله مرد میانی را میتوان با عملکردی در نقش یک پراکسی سرور و معرفی خود به عنوان کاربر مورد اطمینان به هر دو طرف تشخیص داد. یک حمله مرد میانی رمزنگاری نشده قابل تامل، توسط یکی از نسخههای رهیاب شبکه بیسیم Belkin در سال ۲۰۰۳ (میلادی) انجام شد . به گونهای که به صورت تناوبی، روی یک اتصال پروتکل انتقال ابرمتن (HTTP) که برای مسیریابی استفاده میشد انجام شد . این حمله ترافیک را به سمت مقصد، هدایت نمیکرد . در عوض، خودش به عنوان سرور منتخب پاسخ میداد.

برایان وارنر کارشناس امنیتی میگوید حمله مرد میانی پیشرفته این پتانسیل را دارد تا بر تکنیک کپچاها غلبه کند .

پیادهسازیها

ابزارهای مختلفی برای پیادهسازی این مدل حملات در اختیار هکرها قرار دارد که از آن جمله به موارد زیر میتوان اشاره کرد :

- dsniff – набор утилит для перехвата паролей SSH и SSL.

- Cain and Abel – программа для восстановления паролей, перехвата VoIP-разговоров, декодирования паролей, записанных в кэш, анализа маршрутов и вычисления таблиц ARP.

- Ettercap – программа для перехвата сетевого трафика, поддерживающая активный и пассивный анализ многих протоколов.

- Karma – инструмент для проведения атак типа «злой двойник» (Evil Twin 802.11) на беспроводные точки доступа.

- Sourceforge – программа для перехвата трафика 802.11.

SSLStrip – инструмент для перехвата трафика SSL.

Thoughtcrime – инструмент для перехвата трафика SSL.

- Intercepter-NG – программа для перехвата ARP трафика.

- wsniff – программа для перехвата HTTP трафика.

(Man-on-the-side attack)

دفاع در برابر حملههای مرد میانی

همانگونه که اشاره شد این حملات یک کانال ارتباطی که بیشتر یک روی وایفای است را نشانه میروند . با اینحال اگر به نکات زیر دقت کنید قادر به تشخیص حملات مرد میانی خواهید بود :

پیامهای امنیتی را نادیده نگیرید : یک پیام هشدار امنیتی نشاندهنده یک مشکل جدی است. زمانی که مشخصات گواهینامه امنیتی با سرور هماهنگی ندارد، به این معنا است که در حال تبادل اطلاعات با یک سرور فیشینگ یا سرور قربانی هستند که حمله مرد میانی را اجرا میکند . البته این پیام ممکن است نشان دهد که سرور به شکل درستی پیکربندی نشده است.

وجود پروتکل HTTPS را بررسی کنید : زمانی که قصد اتصال به سایت حساسی را دارید یا در نظر دارید اطلاعات مهمی همچون اطلاعات شخصی یا کارتهای اعتباری را وارد کنید به وجود پروتکل HTTPS در نوار آدرس مرورگر دقت کنید. همچنین، افزونه HTTPS Everywhere نیز میتواند در این زمینه راهگشا باشد .

در زمان بهکارگیری شبکههای وایفای عمومی آگاه باشید : از شبکههای وایفای عمومی استفاده نکنید یا تنها برای انجام کارهای عادی همچون وبگردی از آنها استفاده کنید . در نتیجه برای عملیات بانکداری آنلاین یا ارسال اطلاعات حساس از شبکههای ایمن و شبکههایی که خود روی آنها نظارت دارید (شبکه سلولی موبایل یا وایفای خانگی) استفاده کنید .

از نرمافزارهای ضدویروسی استفاده کنید : نرمافزارهای امنیتی و سایر مکانیزمهای امنیتی با شناسایی موارد مشکوک به شما کمک میکنند تا هرگونه فعالیت مشکوک یا نصب بدافزار روی سامانهها را تشخیص دهید.

در شماره آینده مبحث فوق را ادامه میدهیم .

برای مطالعه رایگان تمام بخشهای دوره **CEH** روی لینک زیر کلیک کنید :

آموزش رایگان دوره CEH

دسته بندی:
امنیت
تاریخ انتشار :
09:50 - 08/06/1399
برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش رایگان CEH10 - هک اخلاقی - حمله مرد میانی - حمله شخص کناری - Man-in-the-middle - Man-on-the-side

---

نشانی
https://www.shabakeh-mag.com/security/17334/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D8%AD%D9%85%D9%84%D9%87-%D9%85%D8%B1%D8%AF-%D9%85%DB%8C%D8%A7%D9%86%DB%8C-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D9%BE%DB%8C%D8%A7%D8%AF%D9%87%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-%D9%85%DB%8C%E2%80%8C%D8%B4%D9%88%D8%AF%D8%9F