شناسایی و مقایسه انواع هکرها به ما کمک می‌کند بیشتر در مقابل آنها ایمن باشیم

کلاه رنگی‌ها

هکرها از مهارت‌های خود برای عبور از امنیت دیجیتال و دسترسی به اطلاعات محدود استفاده می‌کنند. در حالی که آنها اغلب مجرم هستند، انواع مختلفی از هکرها هم وجود دارند که مخرب نیستند. ما در این مطلب تفاوت‌های بین کلاه سیاه، کلاه خاکستری، هکرهای کلاه سفید و انواع کمتر شناخته شده را بررسی می‌کنیم.

هکرها معمولاً براساس قصد، هدف و قانونی بودن عمل طبقه‌بندی می‌شوند، اما تعاریف هکرها همیشه سیاه و سفید نیست.

کلاه سفید

هکرهای کلاه سفید برای بهبود امنیت دیجیتال کسانی که با آنها قرارداد دارند، در فعالیت‌های هک قانونی شرکت می‌کنند. آنها برای نفوذ به سیستم‌های دیجیتال برای شناسایی آسیب‌پذیری‌های امنیتی بالقوه و گزارش یافته‌های خود به مشتریان، دستمزد دریافت می‌کنند.

هک کلاه‌سفیدها به شرکت‌ها و سازمان‌ها اجازه می‌دهد تا نقاط ضعف امنیتی را قبل از اینکه توسط هکرهای مخرب مورد سوءاستفاده قرار گیرند، اصلاح کنند. به‌عنوان مثال، یک شرکت بیمه ممکن است یک هکر کلاه سفید را برای شبیه‌سازی حملات سالانه به‌منظور اطمینان از ایمن بودن اطلاعات شخصی مشتریان خود استخدام کند. هک کلاه سفید براساس رضایت است و مشتریان درخواست می‌کنند و می‌دانند که تلاشی برای هک کردن سیستم آنها انجام خواهد شد.

کلاه سیاه

هکرهای کلاه سیاه مجرمانی سایبری هستند که کلاهبرداری‌ها را سازماندهی می‌کنند و از آسیب‌پذیری‌ها با هدف ایجاد آسیب سوءاستفاده می‌کنند. هدف هکرهای کلاه سیاه معمولاً کسب درآمد است. آنها این کار را به طرق مختلف انجام می‌دهند. بیشتر روش آنها شامل سرقت مستقیم پول و شکستن رمزهای عبور برای دسترسی به اطلاعاتی هستند که می‌توانند در وب تاریک فروخته شوند یا داده‌های حساس را برای باج نگه می‌دارند. کلاه سیاه‌ها خطرناک‌ترین هکرها هستند و معمولاً تمام تلاش خود را می‌کنند تا هویت خود را پنهان کنند. معمولا پیش نمی‌آید که یک هکر آشکارا با شما چت کند. آنها گاهی اوقات در گروه‌های هکری با هم متحد می‌شوند تا هک‌های بزرگ را انجام دهند. هکرهای کلاه سیاه اغلب با هک کردن دستگاه‌های فردی مانند تلفن‌ها و روترها به سیستم‌های بزرگ‌تر دسترسی پیدا می‌کنند. اکانت‌های ایمیل نیز اهداف محبوبی برای آنها هستند. به همین دلیل است که برای کسب‌وکارها انجام آزمایش‌های منظم امنیت سایبری و برای افراد محافظت از داده‌های خود با نرم‌افزار محافظت از تهدید مانند AVG AntiVirus بسیار مهم است.

کلاه خاکستری

کلاه خاکستری در یک منطقه هک اخلاقی مبهم بین سفید و سیاه قرار دارد. این هکرها بدون رضایت اهداف خود به سیستم آنها نفوذ می‌کنند، اما از آسیب‌پذیری‌ها برای ایجاد آسیب سوءاستفاده نمی‌کنند. در عوض آنها به قربانیان هک اطلاع می‌دهند تا به آنها کمک کنند امنیت خود را بهبود بخشند.

اما هکرهای کلاه خاکستری همیشه این اطلاعات را به‌صورت رایگان به اشتراک نمی‌گذارند. در حالی که کلاه خاکستری‌ها به شرکت‌ها اطلاع می‌دهند که هک شده‌اند، آنها گاهی اوقات در ازای جزئیات درخواست هزینه می‌کنند. در این موارد، قربانیان اگر می‌خواهند آسیب‌پذیری‌های سیستم خود را بدانند، باید هزینه پرداخت کنند اما اگر از پرداخت امتناع کنند، هکرهای کلاه خاکستری تلاشی برای تلافی و ایجاد آسیب نخواهند کرد.

هک کلاه خاکستری‌ها به اندازه هک کلاه سیاه‌ها مخرب نیست، اما همچنان فعالیت آنها غیراخلاقی است. هکرهای کلاه خاکستری بدون رضایت به سیستم‌ها نفوذ می‌کنند و حتی اگر هدف آنها بهبود امنیت باشد، اقدامات آنها همچنان غیرقانونی است.

کلاه قرمز

هکرهای کلاه قرمز خود را «اِبَر قهرمانان» دنیای هک می‌دانند. آنها معمولاً هکرهای کلاه سیاه را هدف قرار می‌دهند تا حملات آنها را مختل یا علیه آنها تلافی کنند. در حالی که هکرهای کلاه قرمز به‌شدت ضد کلاه سیاه‌ها هستند، از تکنیک‌های مشابهی برای هک کردن حلقه‌ها یا افراد کلاه سیاه استفاده می‌کنند. آنها ممکن است حملات تمام‌عیاری انجام دهند تا سرورهای کلاه سیاه را از بین ببرند یا منابع آنها را بدزدند و آنها را به کسانی برگردانند که مورد ظلم قرار گرفته‌اند.

کلاه آبی

هکرهای کلاه آبی هکرهای کلاه سفیدی هستند که توسط یک سازمان استخدام می‌شوند. وظیفه آنها حفظ امنیت سایبری سازمان و جلوگیری از حملات است. کلاه آبی‌ها معمولاً زمانی که توسط یک سازمان یا شرکت استخدام می‌شوند، «هکر» نامیده نمی‌شوند.

کلاه زرد

یک هکر کلاه‌زرد روی هک یا سرقت حساب‌های شبکه‌های اجتماعی تمرکز می‌کند. انگیزه آنها انتقام گرفتن از یک فرد یا سازمان یا دستیابی به اطلاعات شخصی است.

کلاه سبز

این اصطلاح به هکرهای بی‌تجربه اشاره می‌کند، اگرچه هکرهای کلاه سبز ممکن است آرزوی تبدیل شدن به کلاه سفید یا سیاه را داشته باشند، در حالی که نیت آنها تقریباً همیشه مخرب است و از بدافزارها توسط هکرهای دیگر برای راه‌اندازی حملات خود استفاده می‌کنند.

اهمیت هک اخلاقی در امنیت سایبری

اهمیت هک اخلاقی در امنیت سایبری بسیار مهم است. حملات سایبری را مدیریت، کنترل و از آن جلوگیری می‌کند و باعث می‌شود که کسب‌وکارها و سازمان‌ها از نقض امنیت دور بمانند و در نتیجه آنها را از پیامدهای مخرب دور نگه می‌دارد. با انجام آزمایش در دنیای واقعی، هکرهای اخلاقی از دیدگاه‌ها و تکنیک‌های هکرهای کلاه سیاه برای یافتن آسیب‌پذیری‌های احتمالی استفاده می‌کنند. سپس آنها سعی می‌کنند قبل از اینکه هکرهای بد از آنها سوءاستفاده کنند، این نقاط ضعف را برطرف کنند.

آینده هک اخلاقی در امنیت سایبری چیست؟

هک اخلاقی آینده روشنی دارد. تا زمانی که حملات سایبری و نقض امنیت افزایش یابد، تقاضا برای هکرهای اخلاقی در حال افزایش است. هک هوش مصنوعی نیز یک خطر بالقوه در آینده است و سیستم‌ها به هکرهای اخلاقی بیشتری نیاز دارند.

چگونه یک نفر می‌تواند یک هکر اخلاقی معتبر باشد؟

توسعه مهارت‌های هک اخلاقی شما بین ۱۸ ماه تا ۶ سال طول می‌کشد. هرچه مهارت‌های مرتبط کمتری داشته باشید، زمان بیشتری برای یادگیری صرف خواهید کرد. گواهینامه Certified Ethical Hacker به شما کمک می‌کند تا تست نفوذ انجام دهید، آسیب‌پذیری‌ها را شناسایی و از حملات سایبری جلوگیری کنید. شما می‌توانید با توجه به ترجیحات و علایق خود دوره مناسب را انتخاب کنید.

هدف وسیله را توجیه می‌کند

هدف هک اخلاقی و امنیت سایبری محافظت از سیستم‌ها و داده‌هاست. با این حال، آنها از روش‌های مختلفی برای نزدیک شدن به آن استفاده می‌کنند. امنیت سایبری استراتژی کلی محافظت در برابر حملات سایبری است، در حالی که هک اخلاقی یک تکنیک خاص است که در آن از استراتژی برای شناسایی فعالانه و رسیدگی به آسیب‌پذیری‌ها استفاده می‌شود. یک هکر اخلاقی باید اطلاعات کاملی در مورد همه سیستم‌ها، شبکه‌ها، کدهای برنامه، امنیت و... داشته باشد تا هک را به طور کارآمد انجام دهد. برخی از این مهارت‌ها عبارتند از: دانش برنامه نویسی، مهارت‌های شبکه‌ای، درک پایگاه داده‌ها، دانش چندین سیستم عامل مانند ویندوز، لینوکس، یونیکس، توانایی کار با ابزارهای مختلف هک موجود در بازار و دانش موتورهای جست‌جو و سرورها.