۱- حملات استراتژیک، چه نوع حملاتی هستند؟

این نوع حملات، معمولاً برای دستیابی و کنترل اطلاعات یک هدف طراحی و برنامه ریزی می شوند. این اطلاعات شامل تکنولوژی ها، نقشه ها، توانایی ها، روال ها و guideline ها می باشند که به منظور بهره برداری استراتژیکی مورد استفاده قرار می گیرند. اینگونه حملات، معمولاً توسط اسپانسرها، رقیب های تجاری و تحت عنوان جرائم سازمان یافته، مورد حمایت قرار می گیرند.

۲- حملات تاکتیکی، چه نوع حملاتی هستند؟

این نوع حملات، معمولاً بصورت تصادفی و با دید خوش بینانه صورت انجام می شوند. اطلاعات یک هدف اغلب برای کسب جایگاه بالاتر در تجارت و یا بدست آوردن جوایز مالی از طریق استفاده از بدافزارها، اکسپلویت ها مورد استفاده قرار می گیرند. این دسته از حملات، بوسیله هکرهای حرفه ای و نفوذی ها صورت می پذیرد.

۳- تفاوت اصلی حملات استراتژیکی و تاکتیکی چیست؟

یکی از مهمترین تفاوت های حملات استراتژیکی و تاکتیکی، انگیزه است. حملات تاکتیکی، یک شبکه ی هدف را به قصد کسب جایگاه بالاتر و بدست آوردن جوایز مالی مورد هجوم قرار می دهند، در صورتی که حملات استراتژیکی، از ترکیب چندین حمله تاکتیکی بر روی چندین شبکه ی هدف به منظور بهره برداری استراتژیکی یا مختل کردن دشمن نسبت به استفاده از منابع اش انجام می شوند.

۴- چند نمونه مثال در مورد حملات استراتژیکی بیان کنید.

۱) ورود پنهانی به زیرساخت های استراتژیکی به منظور به دست آوردن اطلاعات. این زیرساخت ها شامل بزرگراه ها، فرودگاه ها، ایستگاه های قطار و راه آهن، خطوط اتوبوس رانی، کشتیرانی، حمل و نقل جاده ای، مراکز تولید و توزیع نیرو، خطوط لوله نفت و گاز، سیستم های آب رسانی و فاضلاب و ... . ۲) هدف قرار دادن زیرساخت های ارتباطی مانند خطوط تلفن همراه، شبکه های کامپیوتری، رادیو و تلویزیون و ... ۳) بانک ها و مراکز مالی ۴) بیمارستان ها، آتش نشانی، اورژانس و ...

۵- منظور از جاسوسی سایبری چیست؟

هدف از جاسوسی سایبری، بدست آوردن اطلاعات محرمانه بدون کسب اجازه از صاحب آن اطلاعات که شامل افراد شخصی، رقبا، گروه ها، دولت و دشمن هستند، می باشد. این اطلاعات به منظور بهره برداری شخصی، اقتصادی، سیاسی و نظامی مورد استفاده قرار می گیرند. جاسوسی سایبری از طریق متدها و روش هایی بر روی بستر اینترنت، شبکه های درون سازمانی و یا کامپیوترهای شخصی و با بهره گیری از تکنیک های کرکینگ و بدافزارها شامل اسب های تروجان، قابل انجام است.

۶- منظور از جنگ سایبری چیست؟

جنگ سایبری، به عملی می گویند که از یک کشور، به کامپیوترها و شبکه های یک کشور دیگر به منظور تخریب و آسیب زدن نفوذ صورت گیرد. از جنگ سایبری به عنوان پنجمین نوع جنگ یاد می شود. (چهار نوع اول عبارتند از: خشکی، دریایی، هوایی و فضایی). زمانی که از جنگ سایبری سخن گفته می شود، منظور رخداد هایی با تأثیر فراوان بر روی هدف های زیاد است. به عنوان

مثال، قطع جریان برق، قطع خطوط تلفن، قطع کنترل ترافیک هوایی، قطع سرویس های اورژانس و ... نمونه هایی از جنگ سایبری هستند.

۷- در مورد کرم استاکس نت توضیح دهید.

کرم استاکس نت، جزء دسته بندی حملات تاکتیکی به شمار می رود. دولت های آمریکا و اسرائیل به منظور خرابکاری در تأسیسات هسته ای ایران، این بدافزار را طراحی کردند. اگرچه، کشورهای دیگری به جز ایران نیز توسط این بدافزار آلوده شدند. این بدافزار از طریق شبکه اینترنت و همچنین وسایلی چون فلش ها گسترش یافت و بر روی سیستم عامل ویندوز قرار می گرفت. اگرچه هدف اصلی آن، سیستم عامل ویندوز نبود. پس از آلوده کردن سیستم، منتظر PLC های زیمنس می ماند تا این کنترلرها به سیستم متصل شوند. تأسیسات هسته ای ایران نیز از همین کنترلرها استفاده میکنند. پس از نفوذ در کنترلر، آن را آلوده کرده و برنامه های آن را تغییر می داد.

۸- نحوه کار ابزارهای تشخیص آسیب پذیری چیست؟

ابزارهای امروزی، یک باگ واحد را که مسئول چندین نوع آسیب پذیری است، گزارش نمی کنند. بلکه اغلب هر آسیب پذیری را بطور جداگانه برای برنامه نویس گزارش می دهند. در نتیجه برنامه نویس نمیداند دقیقاً مشکل و آسیب پذیری اصلی برنامه در کجا قرار دارد. همچنین در بسیاری از ابزارها، خطاهای منطقی مانند انتخاب session ID تصادفی، گزارش نمی شوند.

۹- در مورد حمله Night Dragon توضیح دهید.

این حمله، در زمره حملات جاسوسی قرار دارد. در سال ۲۰۱۱، McAfee گزارش داد که حملات گسترده و سازماندهی شده ای به کمپانی های بزرگ و اصلی نفت و انرژی صورت گرفته است. بر اساس تحقیقات، انگشت اتهام به سوی چین اشاره داشت. این کمپانی ها در کشورهایی نظیر آمریکا، یونان و تایوان قرار داشتند. حمله کنندگان، از آسیب پذیری سیستم عامل ویندوز، برخی نرم افزارها (آسیب پذیری هایی که منجر به حمله SQL injection می شدند) و Active directory استفاده کردند. اطلاعات به سرقت رفته، شامل اطلاعات عملکردی کمپانی ها، پیشنهادهای کاری و مالی و اطلاعات مالی مربوط به پروژه های آنان بود.

۱۰- حملات ناشناس (anonymous) به چه حملاتی گفته می شود؟

حملات ناشناس، در واقع مجموعه فعالیت هایی هستند که بصورت غیرمتمرکز اجرا می شوند و معمولاً می توان اینگونه تعبیر کرد که ناشی از تحرکات اجتماعی هستند. این تحرکات، بر روی بازه زیادی از اهداف (از اهداف مذهبی مانند کلیساها تا کمپانی هایی مانند Visa، MasterCard، PayPal و تا مؤسسات دولتی در کشورهایی نظیر آمریکا، اسرائیل و ...) صورت می گیرند.