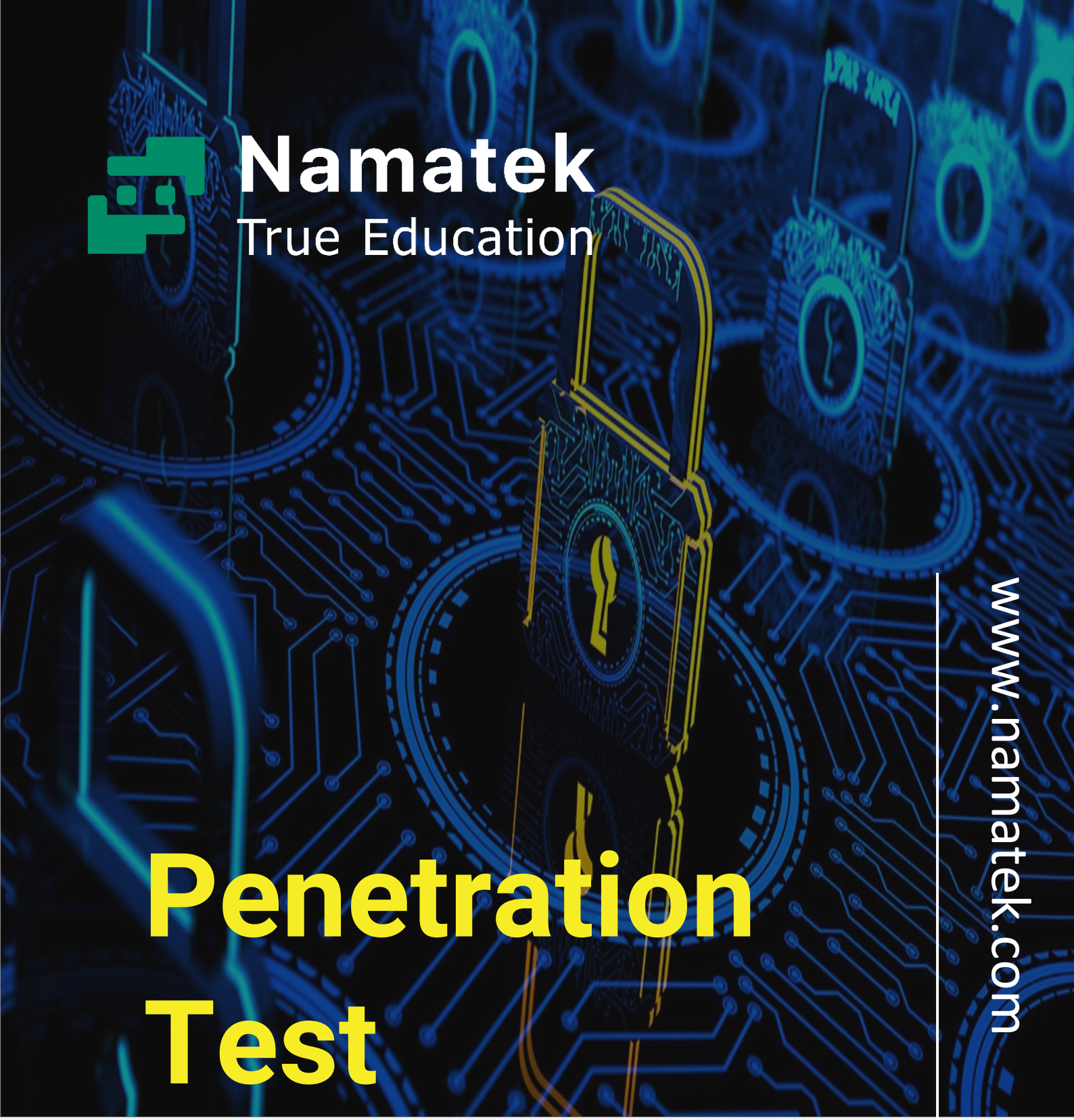


تست نفوذ چیست؟

فهرست مطالب

۱. تست نفوذ چیست؟

۲. مراحل تست نفوذ چیست؟

۳. روش های تست نفوذپذیری

۴. دلیل اهمیت تست نفوذ چیست؟

۵. چه کسی تست نفوذ پذیری را انجام می دهد؟

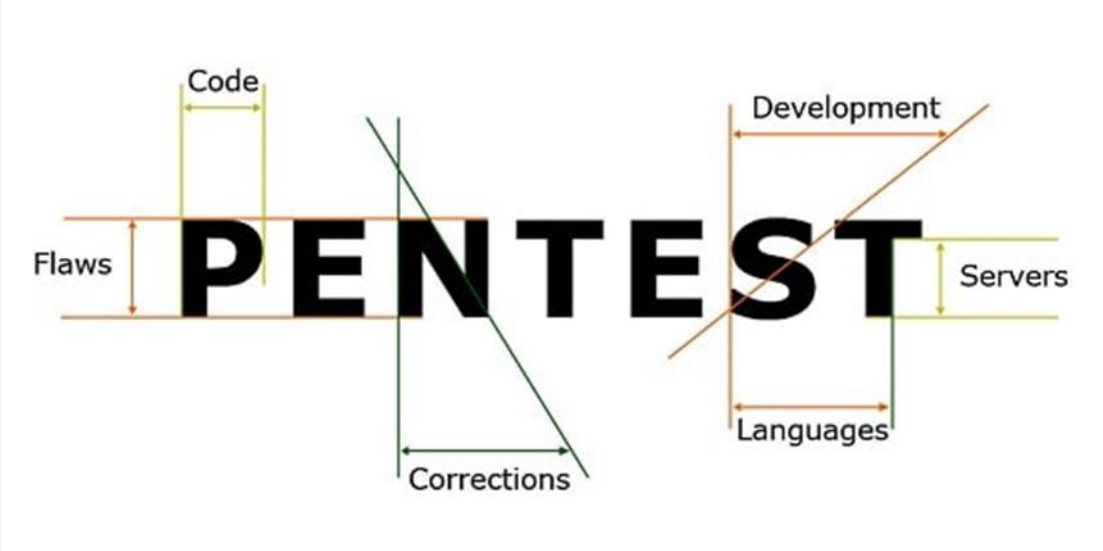
تست نفوذ یک نیاز اساسی برای پیشگیری از مشکلات ناشی از حملات هکرها به برنامه و سرویس های تحت شبکه و وب است؛ اما تست نفوذ چیست و توسط چه کسی انجام می پذیرد؟ این تست چگونه انجام می شود و چه روش ها و استراتژی هایی در آن به کار گرفته می شود؟ برای پاسخ به این پرسش ها و کسب اطلاعات بیشتر در این زمینه، در ادامه با ما همراه باشید.

#۱ تست نفوذ چیست؟

تست نفوذ یا Penetration test که به آن Pen test یا هک اخلاقی (ethical hacking) نیز گفته می شود، یک روش امنیت سایبری است که سازمان ها برای شناسایی، آزمایش و برطرف کردن نقاط آسیب پذیر در وضعیت امنیتی خود استفاده می کنند. این آزمایشات نفوذ، اغلب توسط هکرهای اخلاقی انجام می شود. این اشخاص از استراتژی ها و اقدامات یک مهاجم تقلید می کنند تا قابلیت هک شدن سیستم های رایانه ای سازمان، شبکه یا برنامه های وب را ارزیابی کنند.

در واقع هکرهای اخلاقی، متخصصان فناوری اطلاعات (IT) هستند که از روش های هک برای کمک به شرکت ها برای شناسایی نقاط ضعف احتمالی که امکان نفوذ هکر ها به زیرساخت های خود را فراهم می کند، استفاده می کنند. سازمان ها می توانند با استفاده از روش ها، ابزارها و

رویکردهای مختلف، حملات سایبری شبیه سازی شده را انجام دهند تا نقاط قوت و ضعف سیستم های امنیتی خود را آزمایش کنند.



استراتژی تست نفوذ چیست؟ سه استراتژی اصلی در تست نفوذ وجود دارد که هر یک از آن ها سطح معینی از اطلاعات مورد نیاز برای انجام حمله را به کسانی که مسئولیت تست نفوذ را برعهده دارند ارائه می دهد.

به عنوان مثال:

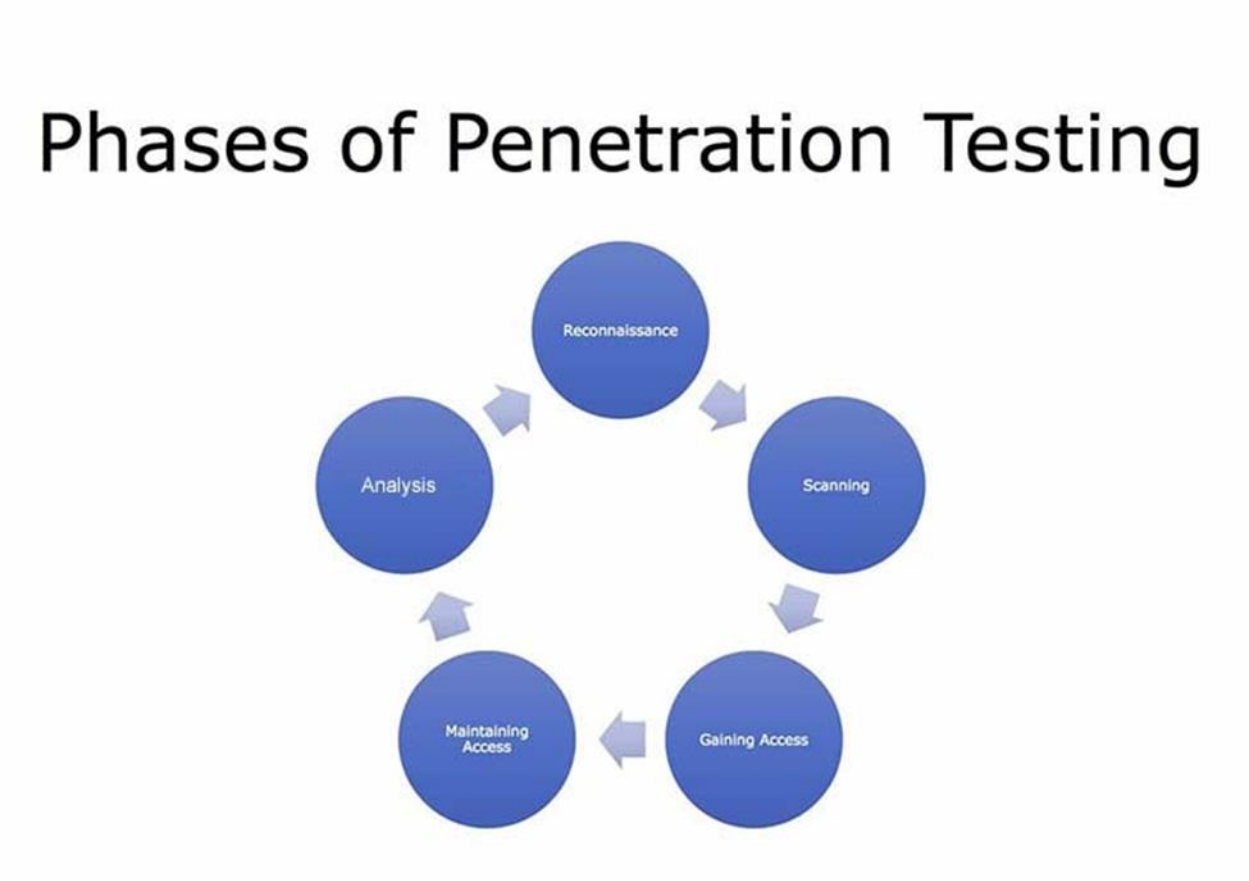
- استراتژی جعبه سفید (white box): تست جعبه سفید تمام جزئیات مربوط به سیستم یا شبکه هدف یک سازمان را ارائه می دهد.
- استراتژی جعبه سیاه (black box): جعبه سیاه هیچ گونه آگاهی از سیستم را در اختیار آزمایش کننده قرار نمی دهد.

- استراتژی جعبه خاکستری (gray box): تست نفوذ جعبه خاکستری دانش جزئی از سیستم را برای آزمایش کننده فراهم می کند.

به طور کلی تست نفوذ به عنوان اقدامی پیشگیرانه در زمینه امنیت سایبری در نظر گرفته می شود؛ زیرا شامل بهبودهای سازگار و مبتنی بر گزارش های تولید شده توسط آزمون است.

#۲ مراحل تست نفوذ چیست؟

فرآیند تست نفوذ را می توان به پنج مرحله تقسیم کرد.



#۲-۱ برنامه ریزی و شناسایی (Planning and reconnaissance)

مرحله اول شامل موارد زیر است:

- تعریف دامنه و اهداف یک آزمون، از جمله سیستم های مورد خطاب و روش های تست مورد استفاده.
- جمع آوری اطلاعاتی مانند نام شبکه و دامنه، سرورهای ایمیل و پایگاه های داده برای درک بهتر نحوه کار، هدف و آسیب پذیری های احتمالی آن.

#۲-۲ اسکن کردن (Scanning)

گام بعدی این است که بفهمید شبکه یا برنامه هدف به تلاش های مختلف جهت نفوذ چگونه پاسخ می دهد.

این کار معمولا با استفاده از موارد زیر انجام می شود:

- تجزیه و تحلیل استاتیک: بررسی کد یک برنامه یا وب سایت تحت وب برای تخمین نحوه عملکرد آن در هنگام اجرای تست نفوذ. این ابزارها می توانند تمام کد را در یک بار اسکن کنند.
- تجزیه و تحلیل پویا: بازرسی کد برنامه در زمان اجرای تست نفوذ. این یک روش عملی تر برای اسکن است؛ زیرا نمای واقعی عملکرد برنامه را فراهم می کند.

#۳-۲ منظور از یافتن دسترسی در تست نفوذ چیست؟ (Gaining access)

در این مرحله از حملات برنامه های وب برای کشف آسیب پذیری های یک هدف استفاده می شود. مانند:

- حمله XSS یا Cross-Site Scripting
- حمله تزریق SQL یا SQL injection
- حمله درهای پشتی یا Backdoor

سپس آزمایش گران تست نفوذ سعی می کنند از این آسیب پذیری ها استفاده کنند و با سرقت اطلاعات، رهگیری ترافیک و غیره، آسیب های ممکن را ایجاد کنند.

#۲-٤ حفظ دسترسی (Maintaining access)

هدف این مرحله این است که ببینیم آیا می توان از آسیب پذیری های دستیابی موجود به صورت مداوم در سیستم استفاده کرد یا خیر؛ زیرا در صورت داشتن دسترسی مداوم ممکن است یک مهاجم از این طریق بتواند به بخش های دیگر نیز دسترسی پیدا کند.

#۵-۲ تجزیه و تحلیل (Analysis)

بخش های مختلف گزارش در تست نفوذ چیست؟ در نهایت، نتایج تست نفوذ در گزارشی با جزئیات کامل در اختیار مدیران و مالکان برنامه قرار می گیرد که برخی از آن ها عبارتند از:

- آسیب پذیری های خاص که مورد سوء استفاده برای نفوذ به سیستم قرار گرفتند
- داده های حساس قابل دسترسی
- مدت زمانی که سیستم قادر به شناسایی تست کننده نفوذ نشده

این اطلاعات توسط پرسنل امنیتی تجزیه و تحلیل می شوند تا به پیکربندی و تنظیمات WAF سازمانی (Web Application Firewall) و سایر راه حل های امنیتی برای از بین بردن یا بهبود آسیب پذیری ها و محافظت در برابر حملات آینده کمک کند.

#۳ روش های تست نفوذپذیری

۱. تست خارجی (External testing): تست نفوذ خارجی معمولا بخش هایی از یک شرکت را مورد هدف قرار می دهد که در اینترنت قابل مشاهده است. به عنوان مثال وب سایت شرکت، برنامه های وب و سرورهای ایمیل و نام دامنه (DNS). هدف، دستیابی و استخراج داده های ارزشمند است.

۲. تست داخلی (Internal testing): در یک تست نفوذ داخلی، یک تستر با دسترسی به یک برنامه در پشت فایروال، حمله یک شخص مخرب در داخل شبکه را شبیه سازی می کند. البته این مهاجم لزوما یک کارمند سرکش نیست و شخص مهاجم می تواند کارمندی باشد که به دلیل حمله فیشینگ مدارک وی دزدیده شده باشد.

۳. تست کور (Blind testing): در یک تست کور، فقط نام سازمانی که هدف قرار می گیرد به یک تستر داده می شود. این امر به پرسنل

امنیتی کمک می کند تا به چگونگی حمله واقعی پی ببرند. در این تست تیم امنیتی از حمله شبیه سازی شده اطلاع دارند؛ اما از جزئیات و نحوه عملکرد آن اطلاعاتی ندارند.

٤. تست دو سو کور (Double-blind testing): تفاوت این روش با روشBlind testing در تست نفوذ چیست؟ در یک آزمایش دو سو کور، پرسنل امنیتی هیچ اطلاعی از حمله شبیه سازی شده ندارند و مانند دنیای واقعی، آن ها از قبل اطلاعی برای دفاع از خود در مقابل حملات نخواهند داشت.

٥. آزمایش هدفمند (Targeted testing): در این سناریو، هر دو آزمایشگر و پرسنل امنیتی با هم کار می کنند و حرکات یکدیگر را ارزیابی می کنند. این یک تمرین آموزشی ارزشمند است که تیم امنیتی بازخورد حمله یک مهاجم را در زمان اجرای آن فراهم می کند.

#۴ دلیل اهمیت تست نفوذ چیست؟

بررسی های اخیر نشان داده است که حملات DDoS، فیشینگ و باج افزار به طرز چشمگیری افزایش یافته و همه شرکت های مستقر در اینترنت را در معرض خطر قرار می دهد. با در نظر گرفتن میزان اهمیت فناوری در کسب و کار های امروزی، پیامدهای یک حمله سایبری برای آن ها بسیار سنگین خواهد بود.

به عنوان مثال یک حمله باج افزار می تواند دسترسی یک شرکت را به داده ها، دستگاه ها، شبکه ها و سرورهایی که برای انجام تجارت به آن ها متکی است، مسدود کند. چنین حمله ای می تواند میلیون ها دلار خسارت ناشی از درآمد از دست رفته داشته باشد. اما در این میان اهمیت تست نفوذ چیست و چگونه به پیشگیری از حملات کمک می کند؟

تست نفوذ با استفاده از دیدگاه هکر، برای شناسایی و کاهش خطرات امنیت سایبری قبل از بهره برداری از برنامه استفاده می کند. این تست به مدیران فناوری اطلاعات کمک می کند تا از اطلاعات امنیتی به روز شده استفاده کنند که احتمال حملات موفقیت آمیز را به حداقل می رساند. علاوه بر این، نوآوری در فناوری یکی از بزرگترین چالش های امنیت سایبری است؛ چرا که با ادامه پیشرفت فناوری، روش هایی که مجرمان اینترنتی استفاده می کنند نیز تغییر می یابد.

برای این که شرکت ها بتوانند با موفقیت از خود و دارایی های خود در برابر این حملات محافظت کنند، باید بتوانند اقدامات امنیتی خود را با همان سرعت به روز کنند. اگرچه اطلاع از روش های صحیح تست نفوذ دشوار است؛ اما با استفاده از هکرهای اخلاقی ماهر، سازمان ها می توانند به سرعت و به طور موثر سیستم خود را که در معرض تکنیک های مدرن هک هستند شناسایی، به روز و جایگزین کنند.

#۵ چه کسی تست نفوذ پذیری را انجام می دهد؟

بهتر است تست نفوذ توسط شخصی انجام شود که در مورد امنیت سیستم بدون دانش قبلی یا کم اطلاع باشد؛ زیرا ممکن است بتواند نقاط کور فراموش شده توسط توسعه دهندگان سازنده سیستم را نشان دهد. به همین دلیل معمولا برای انجام این آزمایشات، پیمانکاران خارجی استخدام می شوند. این پیمانکاران غالبا به عنوان هکرهای اخلاقی شناخته می شوند؛ زیرا آن ها برای هک کردن یک سیستم با اجازه و با هدف افزایش امنیت استخدام شده اند.